Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ETUDE D'IMPACT

PROJET DE LOI

relatif à la protection des données personnelles

NOR : JUSC1732261L/Bleue-1

12 décembre 2017

TABLE DES MATIERES

INTRODUCTION GENERALE

1. Constituant l'une des dimensions du droit au respect de la vie privée, la protection des données à caractère personnel est désormais consacrée comme un droit fondamental à part entière dans la Charte des droits fondamentaux de l'Union européenne (article 8).

La France a toujours été attentive à cette question et a le plus souvent été pionnière. Après avoir été l'un des premiers pays de l'Union européenne à se doter d'une législation globale de protection des données à caractère personnel, avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et d'une autorité de contrôle chargée de veiller à son respect, la Commission nationale de l'informatique et des libertés), notre pays a su, dès 2004 retenir une approche permettant de responsabiliser les organismes mettant en œuvre des traitements de données.

Par le recours au correspondant à la protection des données à caractère personnel ou en confiant de nouvelles missions à la Commission nationale de l'informatique et des libertés comme la certification, l'homologation, la labellisation et la promotion de l'utilisation de technologies protectrices de la vie privée, la France a permis aux différents organismes d'évoluer dans un environnement leur assurant la sécurité juridique tout en protégeant les droits fondamentaux.

2. La protection des données à caractère personnel revêt une dimension particulière depuis l'avènement de l'ère du numérique. Le partage et la collecte de telles données connaissent en effet un développement spectaculaire. C'est par ce biais que les nouvelles technologies transforment aujourd'hui profondément notre l'économie et les rapports sociaux.

Dans le même temps, la protection des données à caractère personnel constitue un motif de préoccupation croissante chez nos concitoyens ; étant entendu qu'une telle préoccupation est largement partagée en Europe. En 2017, 85% des Français se disent ainsi préoccupés par la protection de leurs données personnelles en général, soit une augmentation de quatre points par rapport à 2014. Une question qui suscite encore plus d'inquiétude dès lors qu'il s'agit de la protection des données sur Internet : 90% des personnes interrogées se disent préoccupés pour leurs données mises en ligne, ce qui représente cinq points de progression par rapport à en 2014[1].

3. Devant de telles transformations, il était nécessaire que l'Union européenne prenne les dispositions nécessaires. Dans ce contexte, la Commission européenne a présenté, en janvier 2012 deux projets distincts définissant un nouveau cadre juridique applicable à la protection des données à caractère personnel[2]. La France a pris une part très active dans les négociations afin de maintenir et promouvoir son modèle de protection des données qui constitue encore aujourd'hui une référence en Europe et dans le monde.

[1] « La protection des données personnelles », étude n° 1700780, CSA research, septembre 2017.
[2]COM(2012) 11 final (disponible en ligne : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf)

A l'issue de longues négociations, le Parlement européen et le Conseil ont adopté le « *paquet protection des données* » le 27 avril 2016, fruit d'un compromis entre les Etats membres de l'Union européenne.

Ce paquet se compose :

- d'un **règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement (UE) 2016/679).** Applicable notamment à la matière civile et commerciale, il constitue le cadre général de la protection des données.

Ce règlement abroge la directive 95/46/CE transposée par la loi n° 2004-801 du 6 août 2004 qui avait modifié la loi n° 78-17 du 6 janvier 1978. Il conforte les droits des personnes physiques sur leurs données à caractère personnel déjà garantis dans la loi n° 78-17 du 6 janvier 1978. Il renforce ainsi notamment le droit d'information des personnes, qui disposeront d'informations plus complètes et claires sur le traitement de leurs données, et en crée de nouveaux : droit à l'effacement ou « droit à l'oubli », droit à la portabilité des données.

En outre, le règlement uniformise et simplifie les règles auxquelles les organismes traitant des données sont soumis tout en renforçant les garanties offertes par la loi n° 78-17 du 6 janvier 1978.

Il prévoit en particulier la réduction des formalités préalables pour la mise en œuvre des traitements comportant le moins de risques, avec le passage d'un système de contrôle *ex ante* de la Commission nationale de l'informatique et des libertés par le biais des déclarations et autorisations à un contrôle *ex post* plus adapté aux évolutions technologiques.

Un tel changement de paradigme, reposant sur une logique de responsabilisation des organismes mettant en œuvre des traitements, nécessite une évolution des missions et pouvoirs de l'ensemble des autorités de protection des données de l'Union européenne, la Commission nationale de l'informatique et des libertés en France.

En contrepartie, la Commission nationale de l'informatique et des libertés voit ses pouvoirs de contrôle et de sanctions renforcés avec la possibilité d'infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'organisme concerné.

Dans ce nouvel environnement juridique, la Commission nationale de l'informatique et des libertés devra accompagner plus encore les acteurs. Il s'agit également de créer un cadre juridique sécurisé pour les opérateurs compatible avec la volonté d'attractivité économique de notre territoire.

Les autorités de contrôle devront également coopérer afin de parvenir à une position commune unique pour toute l'Union européenne, gage de sécurité juridique pour les responsables de traitement et d'une application uniforme en matière de protection des données.

Les obligations prévues par le règlement seront également applicables aux opérateurs installés hors de l'Union européenne et offrant des biens et services aux Européens.

Ce règlement est applicable à compter du 25 mai 2018.

- d'une **directive relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (directive (UE) 2016/680**).

La directive s'applique aux traitements de données à caractère personnel mis en œuvre par une autorité compétente à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

La directive n'est pas applicable dès lors que le traitement de données est mis en œuvre pour d'autres finalités ou par une autorité qui n'est pas compétente. La directive n'est pas non plus applicable aux traitements intéressant la sûreté de l'Etat et la défense, qui ne relèvent pas du droit de l'Union.

La directive vise à faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union, et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

Certaines dispositions de la directive sont porteuses d'un changement de philosophie du droit de la protection des données ; d'autres représentent de réelles innovations qui, sans témoigner d'un réel changement de philosophie, imposent d'importantes modifications d'ordre technique.

Les principales innovations de la directive consistent en la création :

- d'un droit à l'information de la personne concernée par les données personnelles traitées en matière pénale ;

- d'un droit d'accès, de rectification et d'effacement s'exerçant par principe de manière directe, alors que la loi actuelle prévoit un exercice indirect de ces droits pour les traitements intéressant la sécurité publique et la police judiciaire.

Elle précise également les conditions applicables aux transferts de données à caractère personnel vers les autres Etats membres, vers les Etats tiers et vers des entités privées au sein d'Etats tiers en instaurant un mécanisme à plusieurs niveaux en fonction du degré « d'adéquation » du niveau de protection des données. Elle prévoit enfin que tous les accords incompatibles avec les règles de protection des données doivent être renégociés ou complétés par des protocoles pour assurer la protection des données à caractère personnel.

Cette directive doit être transposée d'ici le 6 mai 2018.

4. L'articulation entre la directive et le règlement est précisée par le considérant 12 de la directive. Celui-ci indique notamment que relèvent de la directive les traitements concernant des « *activités menées par la police ou d'autres autorités répressives [qui] sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non*». Il précise que *« ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple les activités de police lors de manifestations, de grands événements sportifs et d'émeutes»,* et que *« parmi ces activités figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale ».*

Il indique en revanche, qu'entrent dans le champ d'application du règlement, pour autant qu'ils relèvent du droit de l'Union, les traitements par lesquels *« les États membres [confient] aux autorités compétentes d'autres missions qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ».

5. Au-delà des exigences propres à la mise en conformité avec le droit européen de la protection des données à caractère personnel, le règlement prévoit plus d'une cinquantaine de marges de manœuvre qui permettent aux Etats membres de préciser certaines dispositions ou d'aller plus loin que ce que prévoit le droit européen. Certaines de ces marges de manœuvre permettent de maintenir des dispositions déjà existantes dans notre droit national. D'autres, en revanche, peuvent être mises en œuvre afin notamment de prendre en compte l'évolution technologique et sociétale.

Le rapport annuel du Conseil d'Etat de 2014, intitulé « *Le numérique et les droits fondamentaux* » a souligné la nécessité de repenser la protection des droits fondamentaux afin de mettre le numérique au service des droits individuels et de l'intérêt général.

De même, le rapport d'information déposé par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée nationale a également révélé l'importance des « *incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française* »[3].

6. Le présent projet de loi a pour objet d'assurer la mise en conformité de notre droit national avec ces nouvelles exigences. La Commission européenne pouvant saisir la Cour de justice de l'Union européenne pour défaut de transposition ou pour transposition incorrecte à

[3] Rapport d'information en conclusion des travaux d'une mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française, présenté par Mme Anne-Yvonne Le Dain et M. Philippe Gosselin ? 22 février 2017.

l'expiration du délai de transposition des directives[4], il est donc impératif de respecter les délais de transposition des directives pour lesquelles la France est susceptible d'être condamnée à d'importantes pénalités financières en cas de retard de transposition.

7. La présente étude d'impact ne traite pas de l'ensemble des dispositions du règlement qui sont d'application directe[5] et ne peuvent être recopiées dans le projet de loi. Ainsi, ne sont pas abordés l'impact des dispositions relatives par exemple au délégué à la protection des données ou les droits nouvellement créés (droit à l'oubli, droit à la portabilité des données) qui devront être mises en œuvre par les responsables de traitements dans le champ d'application du règlement. De même, n'est pas abordée la question de l'âge à partir duquel un mineur peut consentir à une offre directe de services de la société de l'information, fixé à 16 ans par le règlement[6], le Gouvernement ayant fait le choix de ne pas faire usage de la marge de manœuvre permettant aux Etats membres d'abaisser cet âge jusqu'à 13 ans.

[4] Article 258 du Traité sur le fonctionnement de l'Union européenne : « *Si la Commission estime qu'un État membre a manqué à une des obligations qui lui incombent en vertu des traités, elle émet un avis motivé à ce sujet, après avoir mis cet État en mesure de présenter ses observations./Si l'État en cause ne se conforme pas à cet avis dans le délai déterminé par la Commission, celle-ci peut saisir la Cour de justice de l'Union européenne.* »

[5] Article 288 du Traité sur le fonctionnement de l'Union européenne : « *(…) Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre. (…)* ».

[6] Article 8 du règlement.

TABLEAU RECAPITULATIF DES TEXTES D'APPLICATION DU PROJET DE LOI

ARTICLES	TEXTES D'APPLICATION	ADMINISTRATION COMPETENTE
Article 1er (6°)	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère de la Justice
Article 4 (4°)	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère de la Justice
Article 5 II (14e alinéa)	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère de la Justice
Article 6 III	Décret en Conseil d'État	Ministère de la Justice
Article 9 I, (2e alinéa)	Décret en Conseil d'État pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés	Ministère de la Justice
Article 9 (I, 7e alinéa)	Arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés,	Ministère de l'Economie et des Finances
Article 11 (2°)	Décret en Conseil d'État après avis de la Commission nationale de l'informatique et des libertés	Ministère de la Justice
Article 13 (15e alinéa)	Décret en Conseil d'État	Ministère des Solidarités et de la Santé
Article 13 (19e alinéa)	Arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés	Ministère des Solidarités et de la Santé
Article 13 (42e alinéa)	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère des Solidarités et de la Santé
Article 15	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère des Armées
Article 19 (30e alinéa)	Décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés	Ministère de la Justice

Article 20	Ordonnance (article 38 de la Constitution)	Ministère de la Justice
	Arrêté	Ministère de la Justice
Article 24		

TABLEAU SYNOPTIQUE DES CONSULTATIONS OBLIGATOIRES

Articles	Objet de l'article	Consultations menées
Ensemble des dispositions du projet de loi		Commission nationale de l'informatique et des libertés Avis du 30 novembre 2017
Article 6	Mesures correctrices et sanctions	
Article 9	Simplification des formalités préalables à la mise en œuvre des traitements	
Article 10	Sous-traitants	Conseil national d'évaluation des normes Avis favorable du 30 novembre 2017
Article 12	Traitements archivistiques	
Article 14	Déclaration administrative automatisée	
Article 17	Dispositions relatives à l'aménagement d'une voie de recours définie par l'arrêt CJUE –C-362/14	Conseil supérieur des tribunaux administratifs et cours administratives d'appel Avis favorable du 7 novembre 2017
Article 17	Dispositions relatives à l'aménagement d'une voie de recours définie par l'arrêt CJUE –C-362/14	Commission supérieure du Conseil d'État Avis favorable du 1er décembre 2017

TITRE I^ER
DISPOSITIONS COMMUNES AU REGLEMENT (UE) 2016/679 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016 ET A LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016

CHAPITRE I^ER
DISPOSITIONS RELATIVES A LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

ARTICLE 1^ER

MISSIONS DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. Cadre général

La Commission nationale de l'informatique et des libertés (CNIL), créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, a été la première autorité administrative indépendante dont la France s'est dotée et l'une des premières à travers le monde en matière de protection des données à caractère personnel.

La Commission nationale de l'informatique et des libertés occupe un rôle central dans la protection des données à caractère personnel en France. Ses missions, prévues à l'article 11 de loi n°78-17, sont les suivantes :

- information des personnes concernées et des responsables de traitement ;
- fonction consultative auprès du Gouvernement ;
- participation à la définition du cadre normatif sur la protection des données personnelles ;
- mise en conformité des traitements ;
- avis, approbation ou création d'instruments de « droit souple » ;
- certification de méthodologies d'anonymisation, notamment en vue de la réutilisation des bases de données publiques mises en ligne ;
- conduite de la réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ;
- promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

1.2. Cadre du droit de l'Union européenne

1.2.1 Le considérant 117 du règlement (UE) 2016/679 et le considérant 75 de la directive (UE) 2016/680 indiquent que l'autorité de contrôle est « *un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel* ». Cette autorité

de contrôle exerce ses missions et pouvoirs en toute indépendance. L'article 41 (3) de la directive prévoit en outre que l'autorité de contrôle instituée au titre du règlement peut également être compétente dans le champ d'application de la directive (UE) 2016/680. Au regard de ces différents éléments, la Commission nationale de l'informatique et des libertés constitue ainsi une autorité de contrôle au sens du « paquet européen » de la protection des données.

1.2.2 Les articles 57 du règlement (UE) 2016/679 et 46 de la directive (UE) 2016/680 prévoient les missions des autorités de contrôle. L'ensemble des missions prévues par la directive se retrouve dans la liste prévue par le règlement à l'exception du g) du 1 de l'article 46 de la directive. Cet exception permet, dans le champ de la directive, à l'autorité de contrôle de vérifier la licéité du traitement et d'informer la personne concernée dans un délai raisonnable de l'issue de la vérification, ou des motifs ayant empêché sa réalisation. D'une manière globale, le règlement est relativement large sur les missions de l'autorité de contrôle dès lors que son article 57(1)v prévoit que cette autorité « *s'acquitte de toute autre mission relative à la protection des données* ». En ce qui concerne la possibilité pour l'autorité de contrôle de prendre des mesures de droit souple, l'article 35.5 du règlement prévoit que : « *L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité* ».

Le présent projet de loi modifie l'article 11 de loi n° 78-17 pour confier à la CNIL de nouvelles missions prévues par le règlement, ou compléter certaines missions déjà exercées.

1.2.2.1. Sur les mesures de droit souple

La Commission nationale de l'informatique et des libertés peut déjà prendre plusieurs mesures de droit souple, ce qui permet de la considérer comme une « autorité de régulation » de la protection des données personnelles. L'article 11 de la loi n° 78-17 prévoit qu'elle peut délivrer des labels[7] et d'une manière générale, « *pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi* »[8].

Comme l'indique M. Jean-Marc Sauvé dans l'avant-propos de l'Etude du Conseil d'Etat sur le droit souple : « *Il semble, tout au contraire, que le droit souple puisse être l'oxygénation du droit et favoriser sa respiration dans les interstices du corset parfois un peu trop serré des sources traditionnelles de la règle. Il peut accompagner la mise en œuvre du "droit dur", comme il peut*

[7] Article 11-3-c) : *« Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label . Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ; »*

[8] Avant dernier alinéa de l'article 11 de la loi n°78-17.

dans certains cas s'y substituer pour la mise en œuvre de politiques publiques suffisamment définies et encadrées par la loi. »[9].

Ainsi, les autorités administratives indépendantes utilisent largement le droit souple, sous forme de recommandations ou de lignes directrices, dans le cadre de leur rôle de régulation.

Pour Mme Isabelle Falque-Pierrotin, présidente de la CNIL[10], le droit souple est nécessaire en matière de protection des données à caractère personnel pour trois raisons :

- compte tenu des limites même de la norme générale dans un environnement en pleine mutation ;
- le traitement des données personnelles est de plus en plus déterritorialisé ;
- la protection des données personnelles est en train de changer de paradigme.

Sur ce dernier point, elle indique, à propos du règlement (UE) 2016/679 : « *initialement, le régime juridique était fondé sur un système relativement binaire : formalités préalables (déclarations, autorisations, etc.) d'une part ; plaintes, contrôles et éventuellement sanctions, d'autre part. Cependant aujourd'hui, face à l'explosion des données personnelles et à leur circulation généralisée, la protection des données personnelles ne peut plus passer uniquement par ces deux volets sauf à accepter une action de régulation limitée et peu efficiente.* »

Parmi les instruments de droit souple, figurent les recommandations qui : « *sans être juridiquement contraignantes par elles-mêmes, précisent les conditions d'application de la loi dans un secteur donné. Si, en règle générale, la CNIL examine chaque situation en tenant compte de ses caractéristiques propres, les recommandations visent une approche plus générale de la règle de droit.* ».

La labellisation permet quant à elle « *à un responsable de traitement qui le souhaite d'obtenir un label "CNIL", à condition de s'engager à respecter une série d'obligations définies par le régulateur, qui vont au-delà de la loi mais lui permettent en retour de se prévaloir de ce haut niveau de conformité à l'égard de ses clients.* »[11] Il est également possible de parler de référentiel.

[9] *Conseil d'Etat, Etude annuelle 2013, « Le droit souple »*, La documentation française, p.5.
[10] « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », dans *Conseil d'Etat, Etude annuelle 2013, « Le droit souple »*, la documentation française, p.5
[11] Ibid, pp. 241 et 242.

1.2.2.2. Sur les règlements types en vue d'assurer la sécurité des systèmes

La CNIL établit et publie actuellement, en application du b) de l'article 11 de la loi n° 78-17, des normes destinées à simplifier l'obligation de déclaration prévue à l'article 23 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes.

Ces règlements types ont la même valeur que les recommandations, instrument de droit souple.

1.2.2.3. Sur la certification

Les certifications, labels et marques permettant d'assurer une certaine transparence des traitements de données à caractère personnel, le processus de délivrance doit lui aussi être transparent (article 42(3) et 43(2)d) du règlement). Ils peuvent parfois être le résultat d'une autorégulation au sein des organismes qui identifient eux-mêmes les limites, la portée de la certification, des labels ou marques.

L'article 42(1) du règlement évoque l'encouragement de la certification par les *« États membres, les autorités de contrôle, le comité et la Commission* » « *[…] aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le règlement […]»*. La certification est en effet volontaire (article 42(3)) et a une durée limitée de 3 ans maximum (article 42(6)).

Ainsi, le règlement confie un pouvoir de certification (directe) aux autorités de contrôle (article 58(3)f). Ce pouvoir de certification permet de certifier des responsables du traitement ou des sous-traitants soumis ou non au règlement (article 42(2)). Il ne s'agit toutefois pas d'un rescrit permettant de certifier le respect du règlement, puisqu' *« une certification [...] ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle qui sont compétentes en vertu de l'article 55 ou 56. »* (article 42(4)).

Le règlement prévoit aussi que les autorités de contrôle approuvent les critères de certification et que les États membres veillent à ce que les organismes de certification soient agréés par l'autorité de contrôle et/ou l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008, en France, le Comité Français d'Accréditation (COFRAC) (article 43(1)). Le législateur national est ainsi tenu de retenir une option, peu importe laquelle.

Dans ce cadre, un mécanisme à deux niveaux est également possible : l'organisme d'accréditation accrédite les certificateurs tiers, qui certifient eux-mêmes divers objets. Dans ce cas, le règlement laisse aux États membres un choix de confier ce pouvoir d'agrément / accréditation soit à la Commission nationale de l'informatique et des libertés, soit à l'organisme national d'accréditation, soit aux deux.

1.2.3. Sur le rôle de conseil de la CNIL auprès des pouvoirs publics

Actuellement, en application du a) du 4 de l'article 11 de la loi n° 78-17 la Commission nationale de l'informatique et des libertés est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Son avis est également requis dans le cadre des régimes d'autorisation prévus aux articles 26 et 27 de la même loi.

L'article 57 du règlement (UE) 2016/679 prévoit que l'autorité de contrôle « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

Le projet de loi prévoit ainsi d'étendre le rôle consultatif de la Commission nationale de l'informatique et des libertés aux propositions de loi, sur saisine du président d'une des deux chambres du Parlement.

1.3. Eléments de droit comparé

Certains Etats membres qui ont déjà adopté une loi de mise en conformité au « paquet européen » de la protection des données, ont également doté, à cette occasion, leur autorité de protection des données de nouvelles compétences.

Par exemple, l'article 14 de la loi allemande sur la protection des données à caractère personnel prévoit un certain nombre de missions « *en plus des missions listées dans le règlement (UE) 2016/679* »[12], telles que :

[12] Section 14 "(1) In addition to the tasks listed in Regulation (EU) 2016/679, the Federal Commissioner shall have the following tasks: \ 1. to monitor and enforce the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;\ 2. to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, paying special attention to measures specifically for children; \ 3. to advise the German Bundestag, the Bundesrat, the Federal Government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data; \ 4. to promote the awareness of controllers and processors of their obligations under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680; \ 5. upon request, to provide information to any data subject concerning the exercise of their rights under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, and if appropriate, to cooperate with the supervisory authorities in other Member States to that end; \ 6. to handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 55 of Directive (EU) 2016/680, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; \ 7. to cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, to ensure the consistency of application and enforcement of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680; \ 8. to conduct investigations on the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from another supervisory authority or other public authority; \ 9. to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial

- promouvoir la sensibilisation et la compréhension du public aux risques, règles, garanties et droits au traitement des données personnelles, en accordant une attention particulière aux mesures spécifiques aux enfants ;

- conseiller le Bundestag allemand, le Bundesrat, le gouvernement fédéral et d'autres institutions et organes sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel ;

- sur demande, fournir des informations concernant l'exercice des droits conférés par la loi allemande relative à la protection des données et, le cas échéant, coopérer avec les autorités des autres États membres à cette fin.

La Belgique[13] ainsi que le Luxembourg[14] ont présenté des projets de loi spécifiques pour leur autorité de contrôle. Pour la Belgique, il s'agit de passer d'un organe d'avis à une autorité de contrôle et de sanction. Une articulation avec les compétences des entités fédérées est prévue. Le Luxembourg semble opérer un renvoi au règlement (UE) 2016/679 sans doter de missions supplémentaires son autorité de contrôle, dans le domaine couvert par le règlement précité.

L'Irlande semble s'orienter vers la création d'une commission (Data Protection Commission), et non plus un commissaire à la protection des données[15].

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. Objectifs poursuivis

La présente disposition ambitionne de maintenir l'efficacité de l'exercice des missions de la Commission nationale de l'informatique et des libertés dans un environnement juridique renouvelé. Dans le cadre de l'harmonisation des règles relatives aux données à caractère personnel au niveau de l'Union européenne et de concurrence internationale, il s'agit de prendre en compte la question de l'attractivité économique et juridique de notre territoire vis-à-vis des opérateurs qui souhaiteraient s'y implanter.

Les nouvelles missions confiées à la Commission doivent lui permettre de maintenir un standard de la protection des données à caractère personnel des personnes tout en répondant à ces nouvelles exigences en termes d'attractivité économique et juridique.

---

practices; \10. to provide advice on the processing operations referred to in Section 69; \ and 11. to contribute to the activities of the European Data Protection Board. \ Within the scope of Directive (EU) 2016/680, the Federal Commissioner shall also perform the task pursuant to Section 60. \ (…)"

[13] https://www.lachambre.be/flwb/pdf/54/2648/54K2648007.pdf

[14] http://www.chd.lu/wps/PA_RoleDesAffaires/FTSByteServingServletImpl?path=/export/exped/sexpdata/Mag/0004/195/9951.pdf

[15] http://www.justice.ie/en/JELR/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf/Files/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf (p.12)

2.2. Nécessité de légiférer

Le présent article du projet de loi modifie l'article 11 de la loi n°78-17 afin de mettre en conformité le droit national avec le règlement (UE) 2016/679 et de transposer la directive (UE) 2016/680.

Cette disposition procède également à quelques modifications nécessaires au regard de la pratique actuelle de la Commission nationale de l'informatique et des libertés.

3. OPTIONS ENVISAGEES

3.1. Inscrire la mesure dans un chapitre commun

L'existence de deux textes (règlement et directive) aurait pu conduire le législateur à voter deux lois distinctes ou à prévoir une séparation stricte des missions de « l'autorité de contrôle » selon qu'il s'agit du champ d'application du règlement ou de celui de la directive.

Toutefois, l'article 41 (3) de la directive prévoit que l'autorité de contrôle instituée au titre du règlement peut également être compétente dans le champ d'application de la directive (UE) 2016/680. L'article 1er du projet de loi précise expressément que la CNIL est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679.

En outre, la Commission nationale de l'informatique et des libertés a été instituée en 1978 pour connaître de l'ensemble des traitements de données, quelles que soient leurs finalités. Certains traitements qui ne relèvent pas du droit de l'Union européenne doivent pouvoir également faire l'objet de contrôle de la part de la Commission.

Pour les raisons évoquées précédemment, le Gouvernement a décidé de maintenir une compétence de la Commission nationale de l'informatique et des libertés à l'égard de l'ensemble des traitements, quels que soient les domaines dont ils relèvent.

3.2. Etendue des missions de la Commission nationale de l'informatique et des libertés

3.2.1. Option 1 (écartée) : se borner à une mise en conformité *a minima* par rapport au règlement et à une transposition de la directive

La Commission nationale de l'informatique et des libertés est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679. Il est proposé de le rappeler par mesure de clarté.

Le règlement confie un pouvoir de certification (directe) aux autorités de contrôle (article 58.3.f[16]). Le règlement prévoit aussi que les Etats membres peuvent retenir en plus un mécanisme à deux niveaux dans lequel un organisme d'accréditation accrédite les certificateurs tiers, qui certifient eux-mêmes divers objets : dans ce cas, le règlement laisse aux Etats membres un choix de confier ce pouvoir d'agrément / accréditation soit à l'autorité de contrôle, soit à l'organisme national d'accréditation (en France, le Comité Français d'Accréditation (COFRAC)), soit aux deux (article 43.1 du règlement[17]). Le règlement prévoit donc une marge de manœuvre qui est précisée, de façon souple, par le nouvel alinéa f bis) de l'article 11. Il est précisé que la commission peut établir des exigences supplémentaires aux normes d'accréditation.

Par ailleurs, afin d'être agréés, les organismes de certification doivent démontrer leur indépendance et leur expertise au regard de l'objet de la certification (article 43(2)a du règlement), respecter les critères fixés par l'autorité de contrôle (article 43(2)b)), mettre en œuvre des procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification (article 43(2)c)), établir des procédures et des structures pour traiter les réclamations et démontrer que leurs tâches et leurs missions n'entraînent pas de conflits d'intérêts.

L'autorité de contrôle (article 58(2)h)) garde toutefois la possibilité de retirer une certification ou ordonner à l'organisme de certification de retirer une certification, ou lui ordonner de ne pas en délivrer si les exigences applicables à la certification ne sont pas ou plus satisfaites.

La Commission nationale de l'informatique et des libertés doit aussi pouvoir agréer / faire accréditer par le Comité Français d'Accréditation (COFRAC)[18] des tiers certificateurs, et concernant les processus d'anonymisation. Il s'agit du renvoi du point 2 g) au point 2 f bis) créé.

---

[16] Article 58.3. « *Chaque autorité de contrôle dispose de tous les pouvoirs d'autorisation et de tous les pouvoirs consultatifs suivants : […] : f) délivrer des certifications et approuver des critères de certification conformément à l'article 42, paragraphe 5* » ;

[17] Article 43.1 : « […] *Les États membres veillent à ce que ces organismes de certification soient agréés par une des entités suivantes ou les deux : a) l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56; \ b) l'organisme national d'accréditation désigné conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56* ».

[18] Le COFRAC, créé en 1994 sous le régime d'une association de droit privé à but non lucratif, a été désigné comme unique instance nationale d'accréditation par le n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, habilité à délivrer des certificats d'accréditation aux organismes d'évaluation de la conformité, que cette accréditation soit obligatoire ou non.

Il est proposé d'indiquer, afin de se conformer aux articles 57.1.c[19] du règlement et 46.1.c[20] de la directive que la Commission nationale de l'informatique et des libertés puisse également être consultée par le Président de l'Assemblée nationale ou par le Président du Sénat sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données.

Ainsi que souligné ci-dessus, la directive prévoit une mission particulière au g) du 1 de l'article 46 de la directive par rapport au règlement et qui n'est pas déjà prévue par la loi n° 78-17. Cette disposition implique une modification du h) du 1 de l'article 11 de cette loi afin d'inclure cette mission qui permet à la Commission nationale de l'informatique et des libertés de répondre à une demande de la personne concernée en cas de restriction de ses droits.

Le projet de texte propose de ne pas se limiter à ces modifications obligatoires.

3.2.2. Option 2 (retenue) : Confier d'autres missions à la CNIL, en sus de celles nécessaires à la mise en conformité au « paquet européen de protection des données » pour prendre en compte la pratique

En plus des trois missions évoquées ci-dessus, il est proposé de rappeler expressément les mesures de droit souple à la disposition de la Commission nationale de l'informatique et des libertés (lignes directrices, recommandations ou référentiels) destinées à faciliter la mise en conformité et l'évaluation préalable des risques par les responsables de traitement et des sous-traitants. Il est également prévu que la Commission encourage l'élaboration des codes de conduite et homologue et publie des méthodologies de référence destinés à favoriser la conformité des traitements de données de santé.
Ces mesures de droit souple ont vocation à fixer un cadre pour certaines catégories de traitements relativement courants et de faciliter les démarches des organismes, en particulier des PME/PMI[21].

Ces mesures doivent permettre d'accompagner les responsables de traitement dans leur démarche de conformité en leur permettant de se « situer » au regard du niveau d'exigence attendu d'eux ; de fonder, le cas échéant, des dispenses d'analyse d'impact, pour des traitements conformes au référentiel[22] ; de permettre l'évaluation du risque résiduel après étude d'impact afin d'aider les responsables de traitement à déterminer s'ils sont ou non soumis à l'obligation de consultation

[19] Article 57.1.c : « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement;* »
[20] Même rédaction que ci-dessus.
[21] Le considérant 98 du règlement précise à cet égard que : « *Il y a lieu d'encourager les associations ou autres organismes représentant des catégories de responsables du traitement ou de sous-traitants à élaborer des codes de conduite, dans les limites du présent règlement, de manière à en faciliter la bonne application, compte tenu des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises. Ces codes de conduite pourraient, en particulier, définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque que le traitement peut engendrer pour les droits et libertés des personnes physiques* ».
[22] L'article 35.5 du règlement prévoit que « *L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité* »

préalable de la Commission nationale de l'informatique et des libertés en application de l'article 36 du règlement.

Le 2 b) de l'actuel article 11 est modifié pour supprimer les normes simplifiées, conséquence de la suppression du régime de la déclaration.

En outre, au-delà des mesures de droit souple, la Commission nationale de l'informatique et des libertés disposera de la possibilité d'établir des règlements types pour assurer la sécurité des systèmes de traitement et de régir les traitements des données de santé (chapitre IX). Elle pourra prescrire des règles d'ordre techniques et organisationnelles sauf pour les traitements mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, pour renforcer les conditions de traitement des données biométriques, génétiques et de santé conformément à l'article 9.4 du règlement (UE) 2016/679 et des garanties complémentaires en matière de traitement de données d'infraction conformément à l'article 10 du règlement (UE) 2016/679.

Enfin, la Commission nationale de l'informatique et des libertés pourra présenter des observations toutes les juridictions à l'occasion de litiges relatifs à l'application du règlement et de la loi n°78-17 (cf. infra, articles du projet de loi relatifs aux voies de recours).

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. Impacts juridiques

La présente disposition modifie la rédaction de l'article 11 de la loi n° 78-17 pour conférer à la Commission nationale de l'informatique et des libertés de nouvelles compétences.

Il en est ainsi des certifications et agréments qu'elle pourra délivrer, le cas échéant, conjointement avec le Comité Français d'Accréditation (COFRAC).

Si la plupart des instruments de droit souple que la Commission nationale de l'informatique et des libertés sera amenée à prendre ne sont dotés d'aucune force contraignante, ils permettent toutefois d'orienter les comportements des responsables de traitement.

Ainsi, une recommandation de la Commission qui se borne à donner une interprétation de la loi n° 78-17 ne constitue pas un acte faisant grief et est, par suite, insusceptible de recours (CE 27 septembre 1989, SA Chopin et Cie, n^{os} 74548, 74549 et 74550)[23].

D'autres instruments constituent en revanche des actes juridiques contraignants, tels que les prescriptions techniques et organisationnelles concernant les traitements des données biométriques, génétiques et de santé et les traitements de données d'infraction que la Commission pourra adopter.

[23] Tel n'est pas le cas en revanche d'une recommandation qui ne se borne pas à commenter les règles dont la CNIL doit assurer le respect mais qui ajoute à l'ordonnancement juridique (CE, sect., 30 octobre 2001, Association française des sociétés financières et a., n° 204909).

La procédure législative est également concernée par ces modifications. En effet, le Président de l'une des deux chambres du Parlement pourra désormais consulter la Commission nationale de l'informatique et des libertés sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données, à l'instar de l'article 4 *bis* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires qui prévoit que le président d'une assemblée parlementaire peut saisir le Conseil d'Etat d'une proposition de loi déposée par un membre de cette assemblée, avant l'examen de cette proposition en commission.

Enfin, la capacité de la CNIL d'agir en justice est renforcée dans la mesure où elle pourra présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement (UE) 2016/679 et de la présente loi.

4.2. Impacts sur les particuliers

L'impact de la certification sur les personnes concernées varie selon le label ou la marque.

Ainsi que le précise le considérant 100 du règlement, afin de favoriser la transparence et le respect du règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

Un label clair et transparent pourra faciliter l'information des personnes sur le traitement des données à caractère personnel les concernant.

4.3. Impact sur les entreprises

Le renforcement des mesures de droit souple que peut prendre la Commission nationale de l'informatique et des libertés est destiné à garantir une meilleure application du droit de la protection des données à caractère personnel et d'offrir aux responsables de traitement, en particulier pour les PME, un cadre juridique sécurisé.

En effet, les représentants des acteurs du numérique (associations, entreprises) ont indiqué que ne pas se sentir encore prêts pour l'application du règlement et des nouvelles obligations qui leur incomberont. L'action combinée du Gouvernement et de la CNIL devra donc leur permettre de comprendre leurs droits et de mettre en œuvre les obligations prévues par les textes européens.

A cet égard, l'article 40 du règlement prévoit que : « *Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises* ». De même, en matière de certification, l'article 42 précise que : « *Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.* ».
La certification ne diminue pas la responsabilité du responsable de traitement (article 42(4) du règlement). Elle a cependant un impact à l'égard des personnes concernées et du public : les responsables de traitements ou les sous-traitants peuvent voir leur image valorisée. La certification aura un impact différent selon l'organisme concerné. Elle permet toutefois de

s'assurer que le niveau de protection des données apporté est plus important, rassurant ainsi sur le risque encouru. A titre d'exemple, dans une étude réalisée en 2016[24], certains organismes décrivent la norme ISO 27001 (Management de la Sécurité de l'Information) comme ayant permis selon eux d'améliorer la sécurité de leur organisme, leur information en la matière, de gagner un avantage compétitif, d'assurer une conformité légale voire même d'obtenir de nouveaux contrats.

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.
Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du projet de loi renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 1er (6°)	Décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés	La Commission nationale de l'informatique et des libertés agrée des organismes certificateurs le cas échéant, de leur accréditation ou concourt à leur agrément par l'instance nationale d'accréditation, mentionnée à l'article 43(1) b du règlement (UE) 2016/679.

[24] http://www.itgovernance.co.uk/iso27001-global-report-2016.aspx

ARTICLES 2 et 3

COMMISSAIRE DU GOUVERNEMENT ET MEMBRES DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. CADRE GENERAL

- **Sur la composition de la Commission nationale de l'informatique et des libertés**

L'article 13 de la loi n° 78-17 relatif à la composition de la Commission nationale de l'informatique et des libertés prévoit que, parmi ses dix-huit membres, cette dernière compte :

- trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;

- deux personnalités qualifiées pour leur connaissance du numérique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat.

Avant la loi n° 2004-801 du 6 août 2004, la notion de personnalité qualifiée n'était appliquée qu'aux deux personnes nommées par décret sur proposition respectivement du président de l'Assemblée nationale et du président du Sénat. Les trois autres personnalités étaient désignées, en raison de leur autorité et de leur compétence, par décret en Conseil des ministres.

La substitution du terme « numérique » à celui d'« informatique », plus représentatif de l'évolution des nouvelles technologies, est intervenue suite à un amendement voté dans le cadre du projet de loi pour une République numérique.

- **Sur le commissaire du Gouvernement auprès de la Commission nationale de l'informatique et des libertés**

Le commissaire du Gouvernement représente le Gouvernement auprès de la Commission nationale de l'informatique et des libertés. Le statut et les missions de ce dernier sont prévus à l'article 18 de la loi n° 78-17.

Présent à l'ensemble des séances de la Commission en formation plénière, il a ainsi compétence pour présenter en séance toute observation reflétant le point de vue du gouvernement sur un projet de délibération.

L'ensemble des dispositions relatives au commissaire du Gouvernement (modalités d'information, présence, etc.) vaut pour toutes les délibérations de la Commission, qu'elles concernent des personnes publiques ou des personnes privées. Le commissaire du Gouvernement ne peut pas participer au vote sur la délibération, mais il peut provoquer une nouvelle délibération dans les

dix jours. Il assiste enfin aux réunions du bureau, sauf lorsque ce dernier se prononce sur l'éventuelle publicité d'une mise en demeure adoptée par son président.

Les conditions de participation du commissaire du Gouvernent auprès de la Commission nationale de l'informatique et des libertés sont précisées par le décret n° 2005-1309. Son article 77 prévoit notamment que : « *Lors de la séance, le rapporteur peut présenter des observations orales sur l'affaire. Le responsable du traitement et, le cas échéant, son conseil sont invités à présenter des observations orales à l'appui de leurs conclusions écrites. Le commissaire du Gouvernement est invité à donner son avis sur l'affaire. La formation restreinte peut entendre toute personne dont elle estime l'audition utile. Dans tous les cas, le responsable du traitement et, le cas échéant, son conseil doivent pouvoir prendre la parole en dernier. Lorsque la formation restreinte s'estime insuffisamment éclairée, elle peut demander au rapporteur de poursuivre ses diligences. La formation restreinte statue hors la présence du rapporteur et du commissaire du Gouvernement*. »

1.2. CADRE CONSTITUTIONNEL

Dans sa décision du 19 janvier 2017, le Conseil constitutionnel a rappelé qu'il appartient au législateur de fixer les règles relatives à la composition et les attributions ainsi que la détermination des principes fondamentaux de l'organisation et du fonctionnement des autorités administratives indépendantes.

Le Conseil constitutionnel est par ailleurs vigilant sur les garanties d'impartialité des autorités administratives indépendantes au regard notamment de leurs pouvoirs de sanction. Ainsi, dans sa décision n° 2012-280 QPC du 12 octobre 2012, Société Groupe Canal Plus et autre, le Conseil constitutionnel a rappelé que les dispositions relatives à la composition, aux règles de délibération et aux modalités de saisine de l'Autorité de la concurrence doivent respecter les principes d'indépendance et d'impartialité découlant de l'article 16 de la Déclaration de 1789.

1.3. CADRE CONVENTIONNEL

L'article 53 (2) du règlement (UE) 2016/679 précise que : « *Chaque membre a les qualifications, l'expérience et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de ses fonctions et de ses pouvoirs*. »

Le choix d'unifier les connaissances requises pour l'ensemble des personnalités qualifiées des membres de la Commission nationale de l'informatique et des libertés en incluant la protection des libertés individuelles à celles-ci s'accorde parfaitement à cet article.

1.4. ELEMENTS DE DROIT COMPARE

La fonction du commissaire du Gouvernement auprès de la Commission nationale de l'informatique et des libertés, autorité de contrôle en matière de protection des données, constitue une spécificité nationale qui n'a pas d'équivalent dans les autres Etats membres de l'Union européenne.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

L'article 2 du projet de loi vise à clarifier les compétences requises pour être une personnalité qualifiée de la Commission nationale de l'informatique et des libertés. Il s'agit également d'une mesure de cohérence entre les personnalités qualifiées désignées par le Président de l'Assemblée nationale et le Président du Sénat et celles désignées par le Gouvernement.

L'article 3 poursuit l'objectif d'alléger la présence du commissaire du Gouvernement aux délibérations de la Commission nationale de l'informatique et des libertés en formation restreinte afin qu'il puisse se consacrer d'autant plus à sa mission d'information auprès des administrations pour que les prescriptions en matière d'informatique et libertés soient correctement comprises et appliquées.

Les modifications apportées par cet article sont également guidées par le souci de rehausser au niveau de la loi les garanties d'impartialité exigées par la jurisprudence constitutionnelle à propos du pouvoir de sanction des autorités administratives indépendantes, avec un double objet :

- prévoir d'une part que le commissaire du Gouvernement, s'il peut être présent aux séances de la formation restreinte compétente pour prononcer des injonctions ou imposer des sanctions, ne peut assister au délibéré qui les suit ;

- exclure d'autre part de ce délibéré les agents de la commission, à la seule exception de ceux chargés du secrétariat de la séance.

2.2. NECESSITE DE LEGIFERER

L'article 2 du projet de loi permet d'unifier le standard de qualifications nécessaires pour être membre de la Commission nationale de l'informatique et des libertés en tant que personnalité qualifiée.

L'article 3 permet de rendre facultative la présence du commissaire du Gouvernement aux délibérations de la Commission nationale de l'informatique et des libertés en formation restreinte uniquement. Cette faculté permettra au commissaire du Gouvernement de consacrer plus de temps à sa mission d'information auprès des administrations pour veiller au respect des délibérations de la Commission nationale de l'informatique et des libertés.
Il s'agit également de tenir compte de la jurisprudence récente du Conseil constitutionnel sur les garanties d'impartialité des autorités administratives indépendantes en prévoyant, dans la loi, que les membres de la CNIL délibèrent hors de la présence des agents de la commission, à l'exception de ceux chargés de la tenue de la séance, et hors de celle du commissaire du Gouvernement.

3. OPTIONS

3.1. ARTICLE 2 : COMPETENCES REQUISES POUR LES PERSONNES QUALIFIEES

3.1.1. Option 1 (écartée) : Maintien du droit existant

Il aurait pu être envisagé de ne pas modifier le droit existant sur les compétences requises des personnalités qualifiées.

La dichotomie de qualifications entre les personnalités qualifiées au sein de la Commission nationale de l'informatique et des libertés, selon qu'elles ont été désignées par les présidents des assemblées parlementaires ou par le Gouvernement, n'apparaît pas satisfaisante car elle pourrait laisser entendre une prédominance du numérique sur la protection des libertés individuelles, ce qui ne correspond pas aux missions de la Commission nationale de l'informatique et des libertés.

3.1.2. Option 2 (retenue) : Unification des connaissances requises pour être désigné en qualité de personne qualifiée

Il n'y a pas lieu de faire de distinction de qualifications selon l'autorité qui désigne la personnalité qualifiée. Par ailleurs, l'ajout de la connaissance des questions touchant aux libertés individuelles comme critère de désignation pour l'ensemble des personnalités qualifiées est cohérent avec les missions de la Commission nationale de l'informatique et des libertés qui protège la vie privée et les données à caractère personnel tout en prenant en compte les évolutions technologiques et leurs impacts (article 11 de la loi n° 78-17).

3.2. ARTICLE 3 : PRECISION DES REGLES RELATIVES AU DELIBERE DE LA COMMISSION

Compte tenu de la jurisprudence récente du Conseil constitutionnel sur les garanties d'impartialité dont doivent disposer les autorités administratives indépendantes dans le cadre de leur pouvoir de sanction, il a été décidé de prévoir expressément dans la loi que, d'une part, les membres de la CNIL délibèrent hors de la présence des agents de la commission à l'exception de ceux chargés de la tenue de la séance, d'autre part, le commissaire du Gouvernement n'assiste pas au délibéré de la formation restreinte de la CNIL.

3.3. ARTICLE 3 : PRESENCE DU COMMISSAIRE DU GOUVERNEMENT AUPRES DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

3.3.1. Option 1 (écartée) : Suppression de la fonction de Commissaire du Gouvernement

La suppression de la fonction de commissaire du Gouvernement auprès de la Commission nationale de l'informatique et des libertés aurait pu être envisagée à l'occasion du présent projet de loi.

Toutefois, une telle fonction apparaît pertinente. En effet, le commissaire du Gouvernement permet d'informer la Commission nationale de l'informatique et des libertés sur les intentions du Gouvernement afin que celle-ci délibère en toute connaissance de cause.

Sa présence aux délibérations lui permet de comprendre les raisonnements et les motifs des délibérations de la commission afin de s'assurer que les textes règlementaires respecteront les raisonnements de l'autorité de contrôle dégagés lors de ses délibérations.

Ainsi, la présence du commissaire du Gouvernement aux délibérations de la Commission nationale de l'informatique et des libertés contribue ainsi au renforcement de la protection des personnes et des organismes concernés, objectif visé par la garantie d'indépendance accordée aux autorités de contrôle par le « paquet européen ».

Le commissaire du Gouvernement contribue donc indubitablement à la cohérence et à la qualité des prises de décisions de la Commission nationale de l'informatique et des libertés mais aussi à une meilleure protection du droit à la protection des données à caractère personnel et à la vie privée.

La présence du commissaire du Gouvernement est donc également nécessaire pour assurer la présence de la puissance publique pour suivre le fonctionnement d'une activité qui, même si elle est confiée à une autorité indépendante, est susceptible in fine d'engager la responsabilité de l'Etat.

3.3.2. Option 2 (écartée) : Maintien du droit constant

La modification n'est pas strictement nécessaire au bon fonctionnement de la Commission nationale de l'informatique et des libertés.

Toutefois, la participation obligatoire aux délibérations en formation restreinte de la Commission nationale de l'informatique et des libertés fait peser une charge de travail importante sur le commissaire du Gouvernement, alors même que toutes les délibérations de cette formation ne concernent pas l'activité administrative.

3.3.3. Option 3 (retenue) : Rendre facultative la présence du commissaire du Gouvernement aux délibérations de la Commission nationale de l'informatique et des libertés

Il est proposé de rendre facultative la présence du commissaire du Gouvernement aux délibérations de la Commission nationale de l'informatique et des libertés en formation restreinte. Cette faculté permettra au commissaire du Gouvernement de consacrer plus de temps à sa mission d'information auprès des administrations pour veiller au respect des délibérations de la Commission nationale de l'informatique et des libertés.

Son information sur les délibérations de la Commission nationale de l'informatique et des libertés n'est pas mise en cause par la seule faculté et non plus l'obligation d'y assister puisque les délibérations de la commission sont publiées au journal officiel.

Ainsi qu'il a été précédemment, le commissaire du Gouvernement n'assiste pas en revanche au délibéré de la formation restreinte chargée de prononcer des sanctions.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGÉES

4.1. IMPACTS JURIDIQUES

L'article 2 du projet de loi aura pour effet que les personnalités désignées par les présidents des deux chambres du Parlement le seront au regard de leur connaissance du numérique, mais également des questions touchant aux libertés individuelles.

Concernant l'article 3 du projet de loi, le caractère facultatif et non plus obligatoire de la présence du commissaire du Gouvernement aux séances de la formation restreinte de la Commission nationale de l'informatique et des libertés ou des réunions de son bureau n'aura aucune incidence juridique sur les décisions prises par ces organes. Il en est de même pour la précision dans la loi des garanties d'impartialité déjà présentes dans le décret et respectées par la Commission nationale de l'informatique et des libertés, selon lesquelles la formation restreinte délibère hors la présence des agents de la CNIL et du commissaire du Gouvernement.

4.2. IMPACTS SUR LES PARTICULIERS

L'article 2 du projet de loi améliore la protection des données à caractère personnel. En effet, il sera désormais possible pour les présidents des deux chambres du Parlement de désigner une personnalité qualifiée pour ses connaissances des libertés individuelles ou du numérique, et pas uniquement sur ses connaissances des questions numériques.

5. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

ARTICLE 4

POUVOIRS DE CONTRÔLE DE LA CNIL

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

1.1.1 Avant l'adoption de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'article 21 de la loi n° 78-17 définissait la mission de contrôle de la Commission nationale de l'informatique et des libertés. Cette dernière pouvait notamment : « *par décision particulière, charger un ou plusieurs de ses membres ou de ses agents, assistés, le cas échéant, d'experts, de procéder, à l'égard de tout traitement, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission* ».

1.1.2 Depuis 2004, il est désormais renvoyé à l'article 44 de la loi n° 78-17 relatif aux contrôles par la Commission nationale de l'informatique et des libertés de la mise en œuvre des traitements[25]. Cet article contient quatre sous-divisions.

Le I de cet article prévoit les limites de temps et de lieux relatives aux contrôles que les membres et agents et de la commission peuvent effectuer. Il s'agit de contrôles sur place et sur pièce, qui complètent le contrôle *a priori*, opéré dans le cadre des formalités préalables et permettent soit de constater l'existence de traitements n'ayant pas fait l'objet de telles formalités, soit de s'assurer du respect effectif de la loi par les traitements déclarés ou autorisés. C'est également dans le cadre de ces dispositions que s'exerce le contrôle par la Commission des dispositifs de vidéo protection[26]. Les contrôles sur place ne sont possibles que dans les lieux ou locaux professionnels privés servant à la mise en œuvre d'un traitement de données personnelles, et non dans les domiciles privés. Les pouvoirs de contrôle incluent la possibilité de recueil et de copie, sur place, de tous les renseignements ou documents utiles. Ce pouvoir de contrôle sur place se double de la possibilité pour les membres et agents de la Commission de procéder à des auditions. Il est également prévu une information préalable du procureur de la République en cas de contrôle.

1.1.3 La loi n° 2011-334 du 29 mars 2011 a modifié le II de l'article 44 de la loi n° 78-17 pour tirer les conséquences de décisions du Conseil d'Etat[27], en prévoyant notamment que « *Le responsable de locaux professionnels privés est informé de son droit d'opposition à la visite* », ainsi que l'intervention du juge des libertés et de la détention. Ainsi, le responsable des locaux –

[25] Article 11 2° f : « *Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions* ».

[26] Articles L. 253-2 et L. 253-3 du code de la sécurité intérieure.

[27] CE, 6 novembre 2009 Société Inter confort, n° 304300 et Pro déco, n° 304301.

qui n'est pas nécessairement le responsable de traitement – est informé, avant le début du contrôle, de son droit d'opposition et peut s'opposer à la visite des lieux privés, qui est alors subordonnée à l'autorisation préalable du juge des libertés et de la détention. Lorsque l'urgence, la gravité des faits ou le risque de destruction le justifie, la Commission nationale de l'informatique et des libertés peut toutefois être autorisée par le même juge à visiter les locaux sans information préalable des responsables de ces locaux ni possible opposition de leur part.

1.1.4 La loi n° 2014-344 du 17 mars 2014 a modifié le III de l'article 44 de la loi n° 78-17 afin de permettre, en plus des contrôles sur place et sur convocation, des contrôles en ligne, afin notamment de lui permettre de constater d'éventuelles failles dans les données à caractère personnel.

Par ailleurs, pour compléter ce dispositif, le second alinéa de l'article 21 de la loi 78-17 précise que les personnes interrogées dans le cadre des vérifications faites par la commission sont tenues de fournir les renseignement demandés « *sauf dans les cas où elles sont astreintes au secret professionnel* ». Il est par ailleurs prévu à l'article 44 de cette loi que les agents de la Commission nationale de l'informatique et des libertés ont accès aux « *programmes informatiques et aux données* » et qu'ils peuvent se faire communiquer « *tous documents nécessaires* » mais que cependant seul un médecin peut requérir la communication de données médicales individuelles.

1.1.5 Enfin, il est précisé que les traitements intéressant la sûreté de l'Etat peuvent être exclus des opérations de contrôle (article 44-IV de la loi n° 78-17).

En 2016, la Commission nationale de l'informatique et des libertés a opéré 430 contrôles, dont 100 contrôles en ligne et 94 concernaient les dispositifs de vidéo protection[28].

1.2. CADRE CONSTITUTIONNEL

Dans sa décision du 29 juillet 2004, le Conseil constitutionnel a examiné la constitutionnalité du dernier alinéa de l'article 21 de la loi n° 78-17. Il a jugé que « *dans le silence des dispositions de la loi du 6 janvier 1978 antérieures à la loi déférée, les personnes interrogées par la Commission nationale de l'informatique et des libertés étaient déjà soumises au secret professionnel* » et que « *l'invocation injustifiée du secret professionnel pourrait constituer une entrave passible des peines prévues par l'article 51 nouveau de la loi du 6 janvier 1978* »[29].

1.3. CADRE CONVENTIONNEL

En premier lieu, les articles 57 et 58 du règlement (UE) 2016/679 précisent les missions et pouvoirs des autorités de contrôle, en particulier les pouvoirs d'enquête dont elles disposent. Le point 6 de l'article 58 du règlement prévoit que chaque Etat membre peut prévoir, par la loi, que son autorité de contrôle dispose de pouvoirs additionnels à ceux prévus par le règlement.

[28] Rapport d'activité de la Commission nationale de l'informatique et des libertés, 2016.
[29] Décision n° 2004-499 DC du 29 juillet 2004, cons. 17 et 18.

L'article 90(1) du règlement prévoit en outre une marge de manœuvre pour les États membres en matière d'obligation de secret. Ceux-ci *« peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, en vertu du droit de l'Union ou du droit d'un État membre ou de règles arrêtées par les organismes nationaux compétents, à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes, lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret. ».*

Cette disposition permet de maintenir la plupart des dispositions de l'actuel article 44 de la loi n° 78-17, notamment l'accès aux locaux des responsables de traitement et aux données nécessaires à l'accomplissement des missions de la commission.

En deuxième lieu, dans une décision du 6 novembre 2009, le Conseil d'Etat a jugé, au regard de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales que : « *si le droit au respect du domicile que ces stipulations protègent s'applique également, dans certaines circonstances, aux locaux professionnels où des personnes morales exercent leurs activités, il doit être concilié avec les finalités légitimes du contrôle, par les autorités publiques, du respect des règles qui s'imposent à ces personnes morales dans l'exercice de leurs activités professionnelles ; que le caractère proportionné de l'ingérence que constitue la mise en œuvre, par une autorité publique, de ses pouvoirs de visite et de contrôle des locaux professionnels résulte de l'existence de garanties effectives et appropriées, compte tenu, pour chaque procédure, de l'ampleur et de la finalité de ces pouvoirs* »[30].

Cette décision a notamment conduit le législateur à modifier le II de l'article 44 de la loi n° 78-17. Le projet de loi ne modifie pas non plus les garanties qui entourent la procédure de contrôle sur place : droit d'opposition à la visite des lieux, locaux, enceintes, installations ou établissements qui servent à la mise en œuvre des traitements, exclusion des locaux affectés au domicile privé, contrôle du juge des libertés et de la détention et respect des droits de la défense avec la possibilité pour l'occupant des lieux de se faire assister d'un conseil de son choix. La suite de la procédure reste également contradictoire, puisque le responsable de traitement est mis en mesure de produire des observations quant au procès-verbal dressé par les membres ou agents ayant conduit le contrôle.

En dernier lieu, les articles 55 du règlement et 45 de la directive prévoient que les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle. Le considérant 20 du règlement précise : « *La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions* ».

L'article 4 du projet de loi propose d'apporter cette précision.

[30] CE, 6 novembre 2009 Société Inter confort n° 304300.

1.4 ÉLEMENTS DE DROIT COMPARE

Le projet de loi luxembourgeois prévoit une section sur le secret professionnel auquel sont astreints les membres et agents de l'autorité de contrôle, sans apporter de précision sur les secrets professionnels précisément protégés.

Le projet de loi belge précise, à son article 67 §2, que « (…) *Les informations concernant des données médicales de nature personnelle ne peuvent être communiquées et utilisées que dans le respect du secret médical.* (…)». Des aménagements procéduraux sont également prévus pour le secret professionnel à l'article 78 « (…) *Sauf accord écrit de la personne concernée ou autorisation du juge d'instruction, l'inspecteur général et les inspecteurs ne peuvent, sans la présence d'un représentant de l'ordre professionnel, pénétrer dans les locaux d'un professionnel qui est soumis au secret professionnel et pour qui une règlementation légale est prévue concernant des examens sur place et l'accès à leurs locaux professionnels* ».

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Les objectifs poursuivis à travers les mesures envisagées par cette disposition du projet de loi sont :

- d'une part, une extension et un renforcement des contrôles a posteriori de la Commission nationale de l'informatique et des libertés ;

- d'autre part, une clarification du régime de l'opposabilité des secrets professionnels lors des demandes de communication effectuées dans le cadre de vérification.

2.2. NECESSITE DE LEGIFERER

L'article 44 de loi n° 78-17 contient les dispositions détaillant le contrôle *a posteriori* de la Commission nationale de l'informatique et des libertés. Il se combine actuellement avec les contrôles *a priori* réalisés par la commission dans le cadre des formalités préalables.

Dès lors que le règlement change de paradigme et que le projet de loi épouse la nouvelle logique de responsabilisation en diminuant de façon importante les formalités préalables, il est nécessaire de modifier certaines dispositions de l'article 44 de loi n° 78-17 afin de renforcer l'effectivité des contrôles de la commission.

3. OPTIONS

3.1. Suppression de la précision « usage professionnel » des locaux contrôles

En l'état actuel, les membres de la commission ainsi que les agents habilités ont, en application I de l'article 44 de la loi n° 78-17, accès « *aux locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé* ». La précision de

l'usage professionnel peut conduire à exclure certaines zones telles que des halls d'immeuble ou des couloirs qui comprennent des photocopieuses.

La suppression de la précision concernant l'usage professionnel des locaux au I de l'article 44 de la loi n° 78-17, et l'adaptation du II de cet article, permet d'inclure les parties communes d'immeubles.

Cette modification est permise en application de l'article 58(1)f du règlement qui permet à la Commission nationale de l'informatique et des libertés « *d'obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres.* ».

Cette suppression permet d'accroître l'efficacité des contrôles sur place effectués par la Commission. Comme indiqué précédemment, cette suppression ne remet pas en cause la protection prévue du domicile privé qui reste garantie.

3.2. Précision relative au régime d'opposabilité des secrets professionnels

3.2.1. Option 1 (écartée) : Maintenir le droit existant

Actuellement, la question de l'opposabilité des secrets protégés par la loi, lors de la demande de communication des documents par les membres et agents de la Commission nationale de l'informatique et des libertés, n'est pas traitée expressément dans la loi n° 78-17. Seul l'article 21 prévoit une protection du secret professionnel des personnes interrogées dans le cadre des vérifications faites par la commission.

L'article 44 de la loi n° 78-17 prévoit que les agents de la Commission nationale de l'informatique et des libertés ont accès aux « *programmes informatiques et aux données* » et qu'ils peuvent se faire communiquer « *tous documents nécessaires* », mais que cependant seul un médecin peut requérir la communication de données médicales individuelles.

Cet état du droit peut paraître ambigu. Une première interprétation pourrait indiquer que les agents de contrôle ne peuvent se voir opposer aucun secret, à l'exception du secret médical. Une seconde interprétation conduirait au contraire à considérer qu'en l'absence de disposition prévoyant expressément l'inopposabilité des secrets protégés par la loi aux agents de contrôle, tout secret pourrait leur être opposé (secret bancaire, des affaires, …).

Si aucune difficulté ne semble s'être présentée en pratique, il est toutefois apparu pertinent, compte tenu notamment de l'augmentation du niveau des sanctions prévu par le règlement, d'affirmer expressément l'inopposabilité des principaux secrets auxquels la commission pourrait être confrontée. L'option d'un maintien du droit existant a donc été écartée.

3.2.2. Option 2 (écartée) : Supprimer l'opposabilité du secret médical

Se pose la question de l'opportunité de maintenir l'obligation d'avoir recours à un médecin pour obtenir la communication des données de santé nominatives. Cette procédure, prévue actuellement par le III de l'article 44 de la loi n° 78-17[31], peut s'avérer complexe dans la pratique.

L'absence de nécessité du recours à un médecin ne serait pas inédite dans les textes. La levée du secret médical pour des agents de contrôle n'ayant pas la qualité de médecin est ainsi prévue pour des agents dont la santé publique constitue l'objet même de la mission de contrôle[32].

La même problématique de l'extension de l'inopposabilité du secret médical à des non-médecins s'est rencontrée pour les agents des autorités régionales de santé. Jusqu'à la loi n° 2016-41 du 26 janvier 2016, l'article L. 1435-6 du code de la santé publique réservait aux agents des autorités régionales de santé ayant la qualité de médecin l'accès aux données à caractère personnel nécessaires à l'accomplissement de leur mission. L'article 193 de la loi du 26 janvier 2016 a ouvert cette possibilité à tous les agents des autorités régionales de santé.

Toutefois, le projet de loi ne propose pas la disparition de l'opposabilité complète du secret médical pour les données de santé.

3.2.3. Option 3 (retenue) : Clarification du régime d'opposabilité des secrets professionnels

Il est proposé de clarifier l'état du droit et d'indiquer expressément que le secret ne peut être opposé aux membres et agents de la commission sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, dans certaines situations, le secret médical.

En ce qui concerne le secret médical attaché aux traitements nécessaires aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé, il ne sera plus exigé que ce soit seul un médecin qui puisse requérir la communication des données mais que cette communication ne peut être faite que sous l'autorité et en présence de ce dernier. Ainsi, il s'agit d'un allègement de la procédure tout en maintenant une garantie importante relative au secret médical dès lors que l'agent de la commission sera sous la responsabilité fonctionnelle du médecin.

Enfin, il est précisé que seuls les agents et membres habilités au secret de la défense, conformément au code de la défense, ont accès aux documents contenant des informations relevant de ce régime[33].

---

[31] « *Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé* ».

[32] Voir par exemple récemment l'art. L. 1333-17-1, issu de l'ordonnance n° 2017-45 du 19 janvier 2017, permettant aux inspecteurs de la radioprotection d'accéder *« ils accèdent, à leur demande et dans des conditions préservant la confidentialité des données à l'égard des tiers, aux informations […] qui leur sont strictement nécessaires, sans que puisse leur être opposé le secret médical ou le secret en matière industrielle ou commerciale.* »

Par ailleurs, le projet de loi rappelle, en application du règlement et de la directive, que la commission n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions, permettant ainsi de préserver le secret de l'instruction.

3.3. Possibilité de faire usage d'une identité d'emprunt

La loi n° 2014-344 du 17 mars 2014 susmentionnée a modifié le III de l'article 44 de la loi n° 78-17 afin de permettre, en plus des contrôles sur place et sur convocation, des contrôles en ligne. Ces contrôles sont très utiles et sont appelés à se multiplier. Toutefois, lorsque la Commission nationale de l'informatique et des libertés utilise une adresse électronique @cnil.fr pour exercer des droits, le responsable de traitement peut modifier son traitement uniquement pour les besoins du contrôle.

Il s'agit de prévoir l'utilisation par les agents de contrôle d'une identité d'emprunt, en prévoyant la possibilité de créer une fausse identité d'un utilisateur lambda pour un contrôle effectif. Il est précisé que l'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées, afin de prémunir ces contrôles du risque de contestations fondées sur la violation du principe de loyauté dans la collecte des preuves.

Cette mesure est de nature à renforcer l'efficacité des contrôles en ligne. Actuellement, l'autorité des marchés financiers dispose d'une telle possibilité (article L. 621-10-1 du code monétaire et financier[34]).

Il n'est toutefois pas proposé d'ajouter une disposition sur l'irresponsabilité pénale des agents.

D'une part, parce qu'il n'est pas prévu que les agents de la commission pourront commettre des infractions sur internet, et que le fait d'utiliser une identité d'emprunt pour se connecter à internet ne constitue aucune infraction pénale.

D'autre part, parce que dès lors que la loi permet d'utiliser une identité d'emprunt, à supposer que cela puisse constituer un délit, puisque la loi l'autorise, il ne peut exister aucune responsabilité pénale en application du code pénal.

---

[33] Article 19 de la loi n° 78-17 : « *[…] Ceux des agents qui peuvent être appelés à participer à la mise en œuvre des missions de vérification mentionnées à l'article 44 doivent y être habilités par la commission ; cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi.* »

[34] Article L. 621-10-1 du code monétaire et financier : « *Lorsque les personnes et entités mentionnées au II de l'article L. 621-9 fournissent leurs services sur internet, les enquêteurs et les contrôleurs peuvent, pour accéder aux informations et éléments disponibles sur ces services, faire usage d'une identité d'emprunt sans en être pénalement responsables. / Un décret en Conseil d'Etat précise les conditions dans lesquelles les enquêteurs et les contrôleurs procèdent dans ces cas à leurs constatation*s ».

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

La modification de l'article 44 de la loi n° 78-17 permettra d'étendre et de préciser le champ des contrôles possibles de la Commission nationale de l'informatique et des libertés et le cadre dans lesquels ils s'opèrent.

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 4 (4°)	Décret en conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés	Conditions dans lesquelles les membres et agents habilités de la Commission nationale de l'informatique et des libertés procèdent à l'utilisation d'identité d'emprunt.

ARTICLE 5

PROCEDURE DE COOPERATION DE LA CNIL AVEC LES AUTRES AUTORITES DE CONTROLE

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La loi n° 78-17 du 6 janvier 1978 contient peu de dispositions relatives à la coopération de la Commission nationale de l'informatique et des libertés avec les autorités de contrôle européennes.

L'article 49, tel qu'issu de la loi n° 2004-801 du 6 août 2004 qui transposait la directive 95/46/CE, prévoit que chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre Etat membre et que les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

Cet article prévoit actuellement que la CNIL peut, à la demande d'une autorité exerçant des compétences analogues dans un autre Etat membre, procéder à des vérifications dans les mêmes conditions, selon les mêmes procédures et sous les mêmes sanctions, sauf s'il s'agit d'un traitement de « souveraineté » (traitement qui intéresse la sûreté de l'Etat, la défense ou la sécurité publique) ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté (article 26 de la loi n° 78-17).

1.2. CADRE CONSTITUTIONNEL

Le chapitre VII du règlement (UE) 2016/679 organise une procédure de coopération entre les autorités de contrôle de l'Union européenne. L'article 62.3 prévoit que : « *Une autorité de contrôle peut, conformément au droit d'un État membre, et avec l'autorisation de l'autorité de contrôle d'origine, conférer des pouvoirs, notamment des pouvoirs d'enquête, aux membres ou aux agents de l'autorité de contrôle d'origine participant à des opérations conjointes ou accepter, pour autant que le droit de l'État membre dont relève l'autorité de contrôle d'accueil le permette, que les membres ou les agents de l'autorité de contrôle d'origine exercent leurs pouvoirs d'enquête conformément au droit de l'État membre dont relève l'autorité de contrôle d'origine. Ces pouvoirs d'enquête ne peuvent être exercés que sous l'autorité et en présence de membres ou d'agents de l'autorité de contrôle d'accueil. Les membres ou agents de l'autorité de contrôle d'origine sont soumis au droit de l'État membre de l'autorité de contrôle d'accueil.* ».

La possibilité de prévoir que des agents d'autorités de contrôle étrangères puissent participer à des opérations conjointes avec des agents de la Commission nationale de l'informatique et des libertés doit s'exercer dans le respect du cadre constitutionnel et des exigences liées à la souveraineté nationale de la France.

Dans sa décision du 17 janvier 1980[35], le Conseil constitutionnel a jugé, à propos de la convention franco-allemande additionnelle à la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959, que : « *considérant que la convention franco-allemande n'apporte aucune atteinte à la règle qui découle du principe de la souveraineté nationale, selon laquelle les autorités judiciaires françaises, telles qu'elles sont définies par la loi française, sont seules compétentes pour accomplir en France, dans les formes prescrites par cette loi, les actes qui peuvent être demandés par une autorité étrangère au titre de l'entraide judiciaire en matière pénale; que les garanties de l'indépendance de ces autorités demeurent pour l'accomplissement de ces actes les mêmes que celles dont elles disposent dans l'exécution d'actes analogues demandés par les autorités françaises; que, dans ces conditions, la convention additionnelle n'est pas contraire à l'article 64 de la Constitution* ».

Le Conseil constitutionnel a également jugé, à propos de l'accord de Schengen du 14 juin 1985[36], que : « *Considérant que la procédure de poursuite transfrontalière régie par l'article 41 de la convention et dont les modalités d'exercice ont fait l'objet d'une déclaration du Gouvernement de la République sur le fondement du paragraphe 9 de l'article 41, n'est ni générale, ni discrétionnaire ; que cette procédure n'est applicable qu'à des hypothèses où il y a soit des infractions flagrantes d'une particulière gravité, soit une volonté de la part de la personne poursuivie de se soustraire à la justice de son pays ; que les agents poursuivants ne disposent en aucun cas du droit d'interpellation ; que l'entrée dans les domiciles et les lieux non accessibles au public leur est interdite ; considérant qu'en raison des modalités de son exercice, la procédure de poursuite transfrontalière ne procède pas à un "transfert de souveraineté"* ; ».

En l'espèce, l'intervention prévue des agents d'autorités de contrôle étrangères est subordonnée à l'acceptation des autorités françaises, sauf cas particuliers : flagrance, volonté d'échapper à sa justice nationale etc. Le respect du droit français est un impératif et les autorités étrangères ne bénéficient pas de tous les pouvoirs : pas d'interpellation par exemple. Il s'agit par ailleurs de cas très particuliers pour la coopération policière comme un fait punissable pouvant donner lieu à extradition.

La convention Schengen n'est pas assimilable à la procédure de coopération entre autorités de contrôle en matière de protection des données prévue par le règlement. Il ne s'agit pas de coopération policière ou judiciaire mais d'agents d'autorité de contrôle. La jurisprudence du Conseil constitutionnel sur l'Accord de Schengen porte sur des arrestations, la poursuite par des agents étrangers au-delà de leurs frontières nationales, mais pas sur une coopération entre autorités administratives indépendantes ou des autorités de contrôle concernant des enquêtes de nature administrative.

Sur ce dernier point, la Cour de cassation a jugé, à propos du mécanisme de coopération entre autorités de la concurrence des Etats membres de l'Union européenne, prévu par le règlement (CE) n° 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité, que les dispositions de l'article 22 de ce règlement ne subordonnent pas l'exécution de la mesure d'enquête sollicitée à l'autorisation

[35] Décision n° 80-116 DC du 17 juillet 1980, considérant 4.
[36] Décision n° 91-294 DC du 25 juillet 1991, considérants 38 et 39 ;

préalable d'un juge de l'État pour le compte duquel elle est effectuée, et que l'autorisation et le déroulement de l'enquête sont régis par le droit national applicable dans l'État destinataire de la demande d'assistance sous le contrôle des juridictions compétentes de cet État et qu'il n'appartient pas au juge français d'autoriser ou de contrôler le déroulement de mesures d'enquête sur d'autres territoires que son territoire national[37].

Au regard de ces éléments, l'article 5 du projet de loi prévoit de mettre en œuvre un système d'autorisation de l'autorité nationale (accord préalable de la CNIL), et les agents des autorités de contrôle étrangers seront sous le contrôle de la CNIL. Il s'agit d'un double contrôle par la CNIL et du respect de la souveraineté nationale.

La procédure est unifiée et applicable à l'ensemble des Etats membres de l'Union européenne. Le droit national, lors des contrôles opérés par des agents d'autorités de contrôle étrangères, trouvera à s'appliquer (par exemple, l'interdiction de contrôler un domicile).
En outre, ne sont pas concernés par la procédure de coopération les fichiers de souveraineté (intéressant par exemple la défense nationale).

Le projet de loi ne porte donc pas atteinte à la souveraineté nationale.

1.3. CADRE CONVENTIONNEL

La section 1 du chapitre VII du règlement (articles 60 à 62) est consacrée à la coopération entre les autorités de contrôle. Le considérant 133 précise notamment que : « *Les autorités de contrôle devraient s'entraider dans l'accomplissement de leurs missions et se prêter mutuellement assistance afin de faire appliquer le présent règlement et de contrôler son application de manière cohérente dans le marché intérieur. [...]* ».

Un mécanisme de contrôle de la cohérence est prévu sous l'égide du comité européen à la protection des données qui regroupera l'ensemble des autorités de contrôle des Etats membres de l'Union européenne et le contrôleur européen à la protection des données.

L'ensemble du chapitre VII du règlement, de par son objectif d'une meilleure coopération et cohérence entre les autorités de contrôle, est très détaillé. Peu de marge de manœuvre sont laissées aux Etats membres sur ce point, sauf en matière de définition des pouvoirs d'enquête qui peuvent être confiés aux membres et agents associés aux opérations conjointes.

[37] Cour de cassation, civile, Chambre commerciale, 20 janvier 2015, 13-16.745 13-16.764 13-16.765 13-16.955, Publié au bulletin

1.4 ÉLEMENTS DE DROIT COMPARE

Le projet de loi belge apporte des précisions d'ordre procédural sur le mécanisme de coopération (voir en ce sens l'article 67).

Le projet de loi luxembourgeois prévoit la possibilité pour les membres du collège, les membres suppléants et agents de la commission nationale pour la protection des données (CNPD) de communiquer des informations relevant du secret professionnel aux autorités de contrôle des autres États membres, au comité européen à la protection des données et à la Commission européenne les informations nécessaires à ceux-ci pour l'exercice de leur surveillance, à conditions qu'ils tombent sous un secret professionnel équivalent (article 45).

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

La mise en conformité du droit national doit s'inscrire dans les limites de ce que prévoit le règlement (UE) 2016/679 et permettre une coopération efficace entre les autorités de contrôle des Etats membres de l'Union européenne chargées de la protection des données à caractère personnel.

2.2. NECESSITE DE LEGIFERER

Les relations entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres Etats membres de l'Union européenne nécessitent d'être profondément revues au regard des nouvelles dispositions du règlement (UE) 2016/679.

Des précisions législatives sont nécessaires afin notamment de répartir les rôles entre les formations collégiales de la Commission et son président.

En revanche, l'article 49 bis de la loi n° 78-17, qui concerne les relations entre la CNIL et une autorité de contrôle d'Etats non membres de l'Union européenne, n'est pas modifié par le présent projet de loi.

3. OPTIONS

Bien que le règlement soit directement applicable, il est proposé de modifier l'article 49 de la loi n° 78-17 qui figure dans les dispositions communes du projet de loi, pour préciser les modalités de coopération en dehors du champ d'application du règlement.

3.1. Répartition des compétences au sein de la CNIL en ce qui concerne la coopération (article 49-1)

3.1.1. Option 1 (écartée) : Compétence du collège, du bureau ou de la formation restreinte de la CNIL

Le règlement encadre la procédure de coopération dans des délais courts. A ce titre, il s'agit de savoir qui décide d'inviter d'autres autorités de contrôle à participer à des opérations conjointes décidées par la CNIL ou qui détermine l'étendue de la participation des agents de la CNIL auprès des autorités étrangères.

Il a été exclu de confier cette compétence à des organes collégiaux de la Commission (collège, bureau ou formation restreinte) au regard de la nécessaire réactivité que supposent de telles décisions.

3.1.2. Option 2 (retenue) : Compétence du président de la CNIL

Le projet de loi prévoit que c'est le président de la Commission qui invite les autres autorités de contrôle concernées à participer aux opérations de contrôle conjointes, décide de conduire ou se prononce sur le principe et les conditions de la participation, désigne les membres et agents habilités, et en informe l'autorité requérante.

Il s'agit de répondre ainsi à la nécessité d'une prise de décision rapide que la convocation d'organes collégiaux (bureau, formation restreinte) ne permettrait pas d'assurer systématiquement.

3.2. Participation des membres et agents des autres autorités de contrôle étrangères (article 49-1)

3.2.1. Option 1 (écartée) : Prévoir une simple participation passive des membres et agents des autorités de contrôle étrangères en cas de contrôle sur le territoire français

L'article 62.3 du règlement permet une marge de manœuvre pour déterminer l'étendue des pouvoirs qui peuvent être octroyés aux membres et agents des autorités de contrôle étrangères.

L'option constituant à limiter le rôle des membres ou agents des autorités de contrôle étrangères à une simple présence passive aux côtés des agents de la CNIL semble contraire à l'esprit du règlement qui invite à envisager une procédure intégrée et renforcée.

3.2.2. Option 2 (retenue) : Permettre au président de la CNIL d'habiliter les agents de l'autorité de contrôle étrangère pour exercer tout ou partie des pouvoirs de vérification et d'enquête des agents de la CNIL

Le projet de loi précise, d'une part, que des membres et agents de la Commission nationale de l'informatique et des libertés doivent être présents aux côtés des agents et membres étrangers lors des contrôles. Ils sont ainsi nécessairement soumis aux obligations qui incombent aux membres et agents de la CNIL.

D'autre part, il permet au président d'habiliter, par décision particulière, ceux des membres ou agents de l'autorité de contrôle concernée qui présentent des garanties comparables à celles requises des agents de la CNIL. Les contrôles auxquels participeront ces agents habilités, qui ne disposeront pas de pouvoirs plus étendus que ceux confiés à leurs homologues français, seront exercés sous l'autorité de la CNIL.

3.3. Cas de coopération lorsque la France est autorité chef de file (article 49-3)

Sur les éléments que la formation restreinte doit transmettre aux autres autorités concernées, il a été retenu que la transmission se fasse avant l'audition éventuelle du responsable de traitement, du sous-traitant ou d'un autre organisme par la formation restreinte.

S'agissant de la procédure contradictoire exigée par l'article 6§1 de la convention européenne des droits de l'homme dans le cadre de la procédure de coopération/ cohérence, le projet de loi prévoit que le contradictoire ait lieu selon les mêmes modalités qu'actuellement, c'est-à-dire avant l'audition par la formation restreinte (possibilité de répondre par écrit au rapport notifié) et au cours de l'audition (par oral). En revanche, après l'audition, s'ouvre une phase de délibéré qui, bien qu'élargie aux autres autorités concernées, reste une phase de délibéré interne à l'administration (une administration elle aussi « élargie »). Autrement dit, il n'est pas nécessaire de soumettre au contradictoire les éventuelles objections pertinentes et motivées ni l'avis ou la décision du comité européen de la protection des données.

Sur la participation des autres autorités à l'audience de la formation restreinte : dès lors qu'il y a codécision, les autorités concernées doivent être mises en mesure d'assister (vidéoconférence) ou de prendre connaissance de la teneur de l'audience de la formation restreinte (grâce à un procès-verbal). En revanche il n'a pas semblé nécessaire de prévoir une participation « active » (possibilité de poser des questions à l'organisme). Le règlement semble en effet ériger l'autorité chef de file en « guichet unique »[38], vis-à-vis de l'organisme et de la collégialité des autorités.

[38] La procédure de guichet unique est précisée au considérant 127 du règlement : « *Chaque autorité de contrôle qui ne fait pas office d'autorité de contrôle chef de file devrait être compétente pour traiter les cas de portée locale lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres mais que l'objet du traitement spécifique ne se rapporte qu'à un traitement effectué dans un seul État membre et ne porte que sur des personnes concernées de ce seul État membre, par exemple lorsqu'il s'agit de traiter des données à caractère personnel relatives à des employés dans le contexte des relations de travail propre à un État membre. Dans ces cas, l'autorité de contrôle devrait informer sans tarder l'autorité de contrôle chef de file de la question. Après avoir été informée, l'autorité de contrôle chef de file devrait décider si elle traitera le cas en vertu de la disposition relative à la coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées (ci-après dénommé "mécanisme de guichet unique"), ou si l'autorité de contrôle qui l'a informée devrait traiter le cas au niveau local. Lorsqu'elle décide si elle traitera le cas, l'autorité de contrôle chef de file devrait considérer s'il existe un établissement du responsable du traitement ou du sous-traitant dans l'État membre dont relève l'autorité de contrôle qui l'a informée, afin d'assurer l'exécution effective d'une décision à l'égard du responsable du traitement ou du sous-traitant. Lorsque l'autorité de contrôle chef de file décide de traiter le cas, l'autorité de contrôle qui l'a informée devrait avoir la possibilité de soumettre un projet de décision, dont l'autorité de contrôle chef de file devrait tenir le plus grand compte lorsqu'elle élabore son projet de décision dans le cadre de ce mécanisme de guichet unique.* »

Les conditions dans lesquelles le caractère contradictoire de la procédure est garanti à l'égard du ou des responsables de traitement et sous-traitants et les modalités de communication des pièces du dossier durant la procédure seront définies par un décret en Conseil d'Etat.

3.4. Répartition des compétences au sein de la CNIL lorsque la CNIL sera autorité concernée appelée à se prononcer sur un projet de mesure correctrice que lui transmettra une autre autorité chef de file (article 49-4)

Le schéma proposé repose sur deux principes : d'une part, l'aiguillage est centralisé au niveau du président ; d'autre part, les mesures sont ensuite fléchées, en fonction de leur objet, vers l'organe (président ou formation restreinte) qui aurait été compétent pour prendre la mesure équivalente.

Cet aiguillage est conforme au modèle français répartissant le pouvoir décisionnel entre des organes distincts de la CNIL.

Il est *a priori* nécessaire de prévoir les détails de cette répartition au niveau de la loi. Toutefois, et afin de tenir les délais restreints de réponse à un projet de mesure (4 semaines en application du 3 de l'article 60 du règlement), il conviendra d'envisager, dans le décret d'application, les solutions permettant de donner à la formation restreinte une plus grande souplesse et une plus grande réactivité qu'aujourd'hui.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

La présente disposition modifie l'article 49 de la loi n°78-17 et créé quatre nouveaux articles qui :

- précise la coopération entre la CNIL et les autorités de contrôle des autres Etats membres de l'Union européenne dans le cadre d'opérations conjointes dans le cadre du champ d'application du règlement (UE) 2016/679 (art. 49-1) ;

- précise la coopération entre la CNIL et les autorités de contrôle des autres Etats membres de l'Union européenne pour les traitements relevant des dispositions de la loi n° 78-17 transposant la directive (UE) 2016/680 (art. 49-2) ;

- précise la procédure lorsque la CNIL agit en tant qu'autorité chef de file (art. 49-3) ;

- précise la répartition des compétences au sein de la CNIL lorsque cette dernière agit en tant qu'autorité concernée par un contrôle mené dans un autre Etat membre de l'Union européenne (art. 49-4).

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 5	Décret en conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés	Conditions d'application de l'article 49-3 de la loi n°78-17.

ARTICLE 6

MESURES CORRECTRICES ET SANCTIONS

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La Commission nationale de l'informatique et des libertés dispose d'un pouvoir de sanction prévu au chapitre VII de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, destiné essentiellement à la mise en conformité des responsables de traitement (articles 45 à 49 bis).

En vertu de l'article 45 de la loi n° 78-17, la procédure de sanction devant la CNIL s'articule entre les pouvoirs d'instruction et de mise en demeure du président de la Commission et les pouvoirs de sanction de la formation restreinte.

Lorsqu'un manquement à la loi est constaté, le président de la CNIL peut mettre en demeure le responsable de traitement de se mettre en conformité (article 45-I). La mise en demeure prescrit alors les mesures à adopter, dans le délai qu'elle fixe et qui ne peut être supérieur à trois mois, renouvelable une fois. La mise en demeure ne présente pas le caractère d'une sanction[39]. Cette mise en demeure peut être rendue publique sur décision du bureau. Si, à l'expiration du délai ainsi accordé pour se mettre en conformité, le responsable de traitement ne s'est pas conformé à la mise en demeure, le président de la CNIL peut saisir la formation restreinte (composée de six membres élus par leurs pairs), les membres du bureau ne pouvant plus siéger dans cette formation pour prononcer une sanction (article 45-II).

Le président de la Commission peut toutefois saisir directement la formation restreinte, lorsque le manquement ne peut plus faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure. Dans ce cas, qui correspond notamment à des hypothèses de manquements limités dans le temps et n'appelant pas ou plus de mesures de correction, comme des failles de sécurité, la formation restreinte peut prononcer directement une sanction (article 45-I alinéa 7).

Les sanctions peuvent consister en un avertissement, une sanction pécuniaire d'un montant maximal de 3 millions d'euros depuis la loi pour une République numérique du 7 octobre 2016 (contre 150 000 € auparavant), et/ou, le cas échéant, une injonction de cesser le traitement ou un retrait de l'autorisation accordée (article 47). La décision de sanction peut être rendue publique à l'initiative de la formation restreinte (article 46).

Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat (article 46) qui statue en premier et dernier ressort (article R. 311-1 4° du code de justice administrative).

[39] CE 27 juillet 2012, AIS2, n° 340026.

L'article 45-III de la loi n° 78-17 prévoit également une procédure d'urgence. Dans ce cas, la formation restreinte peut prendre des mesures adaptées telles que l'interruption de la mise en œuvre du traitement ou le verrouillage des données.

En 2016, sur les 430 contrôles effectués, la CNIL a procédé à 82 mises en demeure et infligé 13 sanctions, dont 4 sanctions financières, toutes publiques et 9 avertissements[40].

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel considère que « *le principe de la séparation des pouvoirs, non plus qu'aucun autre principe ou règle de valeur constitutionnelle, ne fait obstacle à ce qu'une autorité administrative indépendante, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dans la mesure nécessaire à l'accomplissement de sa mission, dès lors que l'exercice de ce pouvoir est assorti par la loi de mesures destinées à assurer la protection des droits et libertés constitutionnellement garantis ; qu'en particulier, doivent être respectés le principe de la légalité des délits et des peines ainsi que les droits de la défense, principes applicables à toute sanction ayant le caractère d'une punition, même si le législateur a laissé le soin de la prononcer à une autorité de nature non juridictionnelle ; que doivent également être respectés les principes d'indépendance et d'impartialité découlant de l'article 16 de la Déclaration de 1789* »[41].

Le projet de loi maintient l'articulation actuelle entre les pouvoirs d'instruction et de mise en demeure du président de la CNIL et les pouvoirs de sanction de la formation restreinte.

Le Conseil d'Etat a jugé, à cet égard, que cette séparation des fonctions d'enquête et de poursuite de celles de sanction au sein de la CNIL, compte tenu de la distinction organique entre le président d'une part, et la formation restreinte d'autre part, est conforme aux droits et libertés garantis par la Constitution[42] et ne méconnaît pas les principes d'indépendance et d'impartialité, faute de séparation des fonctions de poursuite et de sanction au sein de la CNIL[43] .

Enfin, il est précisé que la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement de données à caractère personnel effectués par les juridictions agissant dans l'exercice de leur fonction juridictionnelle[44]. Le principe de séparation des pouvoirs et d'indépendance de l'autorité judiciaire sont ainsi respectés.

---

[40] Rapport d'activité de la Commission nationale de l'informatique et des libertés, 2016.

[41] Décisions n° 2012-280 QPC du 12 octobre 2012, Société Groupe Canal Plus et autre (Autorité de la concurrence : organisation et pouvoir de sanction), cons. 16 ; n° 2013-359 QPC du 13 décembre 2013, cons. 3.

[42] CE, 26 mars 2012, Sté Pages jaunes, n° 353193

[43] CE, 12 mars 2014, société Foncia Groupe, n° 354629.

[44] Voir le considérant 20 du règlement : « *Bien que le présent règlement s'applique, entre autres, aux activités des juridictions et autres autorités judiciaires, le droit de l'Union ou le droit des États membres pourrait préciser les opérations et procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et autres autorités judiciaires. La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions.* »

1.3. CADRE CONVENTIONNEL

Le règlement (UE) 2016/679 se caractérise par la mise en place d'une approche de responsabilisation des organismes traitant des données à caractère personnel. Ce règlement prévoit ainsi de passer d'un système de contrôle *ex ante* de la CNIL à un système de contrôle *ex post*. Ce changement de paradigme permettra aux autorités de contrôle de concentrer davantage leurs actions sur la mission de sensibilisation et d'accompagnement des responsables de traitement et de disposer de moyens de contrôle et mesures correctrices plus conséquentes et dissuasives en cas de violation constatée des règles applicables.

L'article 58 du règlement (UE) 2016/679 et 47 de la directive (UE) 2016/680 prévoient les pouvoirs des autorités de contrôle[45] en précisant leurs pouvoirs d'enquête (article 58.1 du règlement) et les mesures correctrices qu'elles peuvent prendre (article 58.2).

L'article 83 du règlement définit les conditions générales selon lesquelles les autorités de contrôle peuvent imposer des amendes administratives. Celles-ci peuvent s'élever jusqu'à 10 millions euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent (20 millions d'euros ou 4 % du chiffre d'affaires en cas de non-respect d'une injonction).

Enfin, l'article 84 du règlement et l'article 57 de la directive prévoient que les Etats membres déterminent le régime des autres sanctions applicables en cas de violations du règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions doivent être effectives, proportionnées et dissuasives.

En outre, ainsi qu'il a été dit précédemment, le projet de loi ne modifie pas la séparation entre les pouvoirs d'instruction et de mise en demeure du président de la CNIL et les pouvoirs de sanction de la formation restreinte. Cette dernière, qui peut prendre des sanctions, est soumise aux exigences qui découlent de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, notamment en termes de respect des droits de la défense et du caractère contradictoire de la procédure[46] .

1.4. ELEMENTS DE DROIT COMPARE

Certains États membres de l'Union européenne ne permettent pas à leur autorité de protection des données d'adopter des mesures correctrices. L'entrée en vigueur du règlement (UE) 2016/679 conduira ces États à modifier les compétences de leurs autorités de contrôle.

Alors que les autorités de contrôle de l'Allemagne, d'Espagne, de la France, de l'Italie ou du Royaume-Uni peuvent déjà adopter des mesures correctrices, certains Etats membres modifient

[45] L'ensemble des pouvoirs prévus par la directive, au 2 de l'article 47 se retrouve dans la liste prévue par le règlement.
[46] CE, 19 février 2008, société PROFIL France, n° 311974.

actuellement les pouvoirs de leurs autorités de contrôle afin de leur attribuer des pouvoirs de sanction à l'image de la Belgique[47] et du Luxembourg[48].

D'autres États membres complètent les pouvoirs dont disposaient déjà leurs autorités actuellement comme l'Allemagne[49] dans le cadre de la loi générale sur la protection des données adoptée en juin 2017 (mais dont les dispositions relatives aux autorités de protection des données relèvent toutefois majoritairement des Länders) ou encore le Royaume-Uni[50].

Le projet de loi organique espagnol renvoie expressément aux pouvoirs prévus aux articles 57 et 58 du règlement (UE) 2016/679[51]. Il n'attribue cependant pas de pouvoirs supplémentaires à l'autorité de protection des données nationale, mais des autorités de protection des données existent au sein des communautés autonomes.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Le présent projet de loi remplace les articles 45, 46, 47 et 48 de la loi n° 78-17 pour permettre à la CNIL de prendre les mesures correctrices prévues par le règlement (UE) 2016/679 ou par la directive (UE) 2016/680 et compléter celles déjà existantes.

Ces dispositions visent principalement à attribuer à la Commission nationale de l'informatique et des libertés le pouvoir d'adopter les mesures correctrices rendues nécessaires par l'application du règlement, et le changement de paradigme qu'il opère.

Il s'agit de maintenir l'efficacité des mesures correctrices de la Commission nationale de l'informatique et des libertés dans le contexte de responsabilisation des acteurs. Il s'agit également de garantir une protection efficace des personnes concernées face aux traitements qui violeraient les dispositions de la loi ou du règlement européen.

Les mesures correctrices envisagées sont attribuées, selon qu'elles ont ou non le caractère de sanction, au président de la Commission nationale de l'informatique et des libertés ou à la formation restreinte de cette Commission. Elles permettront à la Commission d'agir en vue

[47] http://www.lachambre.be/FLWB/PDF/54/2648/54K2648007.pdf

[48] Avant-projet de loi portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. (MEDIAS IOa/2017)

[49] https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1510752756678

[50] https://services.parliament.uk/bills/2017-19/dataprotection.html

[51] http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%A2%7F%8B%99tt%84sm%A3%91

d'assurer le respect de la protection des données à caractère personnel tout en répondant aux nouvelles exigences du règlement.

2.2. NECESSITE DE LEGIFERER

Le règlement met en place une approche de responsabilisation. Ce changement de paradigme nécessite, en contrepartie, d'adapter les missions et pouvoirs des autorités de contrôle, en particulier en matière de sanction.

Le texte proposé, en se conformant au règlement, adapte les mesures correctrices, plus conséquentes et dissuasives en cas de violation constatée des règles applicables.

3. OPTIONS

3.1. Remplacement de l'article 45 de la loi n° 78-17

3.1.1. Option 1 (écartée) : Ne pas prévoir une répartition des compétences entre le président et la formation restreinte en matière de mesures correctrices

Le règlement ne précise pas la réparation des pouvoirs au sein de l'autorité de contrôle.

Dans ces conditions, il aurait pu être envisagé de renvoyer au règlement intérieur de la Commission nationale de l'informatique et des libertés à la répartition des pouvoirs entre la présidence et la formation restreinte. Ce choix n'a pas été fait dans la loi n° 78-17 par le passé, il n'a pas été fait non plus dans le cadre de la loi n° 2017-55 relative aux autorités administratives indépendantes.

Cette possibilité a également été écartée afin de préserver le droit constant, en respectant ainsi la volonté récemment exprimée du législateur. Il s'agit en effet d'un élément important qui permet de définir le régime de poursuite et de sanction au sein de CNIL au regard des exigences constitutionnelles et conventionnelles précédemment rappelées.

3.1.2. Option 2 (écartée) : Procéder à un simple renvoi au règlement

Un simple renvoi aux dispositions de l'article 58.2 du règlement n'apparaît pas suffisant dans la mesure où ce dernier ne précise pas l'articulation qui doit s'opérer au sein de l'autorité de contrôle entre les fonctions d'instruction et de mise en demeure, et celles de sanction.

En outre, il a été décidé de doter la CNIL des mesures correctrices prévues par le règlement, y compris pour les traitements ne relevant pas de ce dernier (c'est-à-dire ceux relevant du champ d'application de la directive et ou qui sont hors du champ d'application du droit de l'Union européenne).

3.1.3. Option 3 (retenue) : Modification de l'article 45 de la loi n° 78-17 en renforçant les mesures que peut prendre la formation restreinte

Le projet de loi confère à la Commission nationale de l'informatique et des libertés la possibilité de prononcer les mesures correctrices de l'article 58.2 du règlement. Il adapte également la terminologie employée aux termes du règlement. Par exemple, le règlement évoque l'injonction de « mettre en conformité » et non la « mise en demeure ».

Le projet de loi précise la répartition des pouvoirs entre la présidence de la Commission nationale de l'informatique et des libertés et la formation restreinte.

Il attribue au président de la Commission nationale de l'informatique et des libertés un pouvoir d'avertissement du responsable de traitement ou sous-traitant qu'il est susceptible de violer le règlement. Il s'agit d'un avertissement qui n'a pas le caractère de sanction comme c'est le cas actuellement.

La formation restreinte peut, quant à elle, prononcer un « rappel à l'ordre » équivalent de l'actuel « avertissement ».

En outre, dans la mesure où l'article 84 du règlement et l'article 57 de la directive permettent de prévoir des sanctions supplémentaires, dès lors que celles-ci sont proportionnées et dissuasives au sens de ces articles par rapport à l'objectif de mise en conformité aux obligations des responsables de traitement[52] il est proposé d'assortir d'une astreinte l'injonction à un responsable de traitement de se mettre en conformité avec la loi ou le règlement (UE) 2016/679 ou de satisfaire aux demandes présentées par une personne concernée en vue d'exercer ses droits. L'astreinte permettra ainsi de faire cesser rapidement l'atteinte aux droits des personnes concernées, alors qu'il pourrait apparaître économiquement rentable à certains organismes de perpétuer des traitements qui ne respectent pas le règlement ou la loi.

D'autres pouvoirs sont ajoutés, comme par exemple la possibilité, non-prévue par le règlement, de retirer la décision d'approbation d'une règle d'entreprise contraignante.

Il est à noter que plusieurs de ces mesures (par exemple le retrait de la certification et le retrait de la décision d'approbation d'une règle d'entreprise contraignante) sont prononcées par la formation restreinte à titre de sanction, sans préjudice de la possibilité pour l'organe qui aura délivré la certification ou la décision d'approbation (formation plénière) de les retirer lorsqu'il constatera (sans visée répressive) que les conditions légales ne seront objectivement plus remplies.

[52] Le considérant 129 du règlement précise à cet égard que : « […] *Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que soit prise toute mesure individuelle susceptible de lui porter atteinte et éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées.* ».

3.2. Remplacement de l'article 46 de la loi n° 78-17 relatif à la procédure d'urgence

3.2.1. Option 1 (écartée) : Ne pas préciser les modalités applicables à la procédure d'urgence

L'articulation entre l'actuelle procédure d'urgence de la loi n° 78-17 devant la formation restreinte et celle prévue à l'article 66 du règlement (qui permet à une autorité de protection des données de se dispenser provisoirement du mécanisme de coopération et de contrôle de cohérence prévu par ce règlement) est apparue complexe.

En effet, ces deux approches diffèrent sur plusieurs points :

- quant à la nature des mesures, puisque l'article 45.II de la loi n° 78-17 prévoit des mesures non-provisoires (comme l'avertissement), alors que l'article 66 du règlement ne permet à l'autorité concernée que de prendre des mesures provisoires ;

- quant au critère de l'urgence, l'article 45 de la loi n° 78-17 mentionne l'urgence à agir en présence d'une violation des droits et libertés, tandis que l'article 66 du règlement évoque des « circonstances exceptionnelles » et une « urgence à intervenir pour protéger les droits des personnes concernées ».

Cette option a donc été écartée.

3.2.2. Option 2 (retenue) : Prévoir une procédure d'urgence propre dans le cadre de la loi nationale

L'option retenue a été de prévoir une procédure d'urgence « de droit commun » pour les cas n'appelant ni coopération ni cohérence entre autorités de contrôle ou pour les procédures hors du champ d'application du règlement.

Le projet de loi prévoit ainsi de maintenir les mesures que peut prendre actuellement la formation restreinte (1°, 2°, 6° et 7° du I de l'article 46 de la loi n° 78-17), en ajoutant d'autres types de mesures correctrices qui seraient susceptibles d'être prononcées dans le nouveau contexte juridique (suspension de la certification ou d'un agrément, suspension provisoire de l'autorisation délivrée au titre du chapitre IX concernant les traitements de données de santé) ou encore qui apparaissent opportunes (injonction).

Les II et III résultent de la nécessité de mettre en œuvre les paragraphes 2 à 4 de l'article 66 du règlement.

Le IV de l'article 46 proposé reprend l'article 45.III actuel de la loi n° 78-17.

3.3. Modification de l'article 47 de la loi n° 78-17

3.3.1. Option 1 (écartée) : Suppression de la publicité des mesures prises par la formation restreinte

Le second alinéa aurait pu supprimer la publication de la mesure prise par la formation restreinte. Cette option a cependant été écartée en raison du caractère dissuasif de cette mesure et de la sensibilisation qu'apporte une telle publication.

3.3.2. Option 2 (retenue) : Maintien du droit existant

Le projet de loi propose de maintenir le droit existant concernant la procédure de sanction (article 46 de la loi n° 78-17).

Le second alinéa prévoit la publicité de la sanction. Cette publicité n'est pas prévue par le règlement mais est ajoutée compte tenu de la marge de manœuvre précitée de l'article 84 du règlement dès lors que la décision de rendre publique la sanction prononcée a le caractère d'une sanction complémentaire[53]. Ce pouvoir permet une meilleure harmonisation du droit. Elle permet également la sensibilisation des personnes concernées, des responsables de traitement et sous-traitant permettant à ces publics de prendre des mesures appropriées pour les traitements de données qu'ils opèrent.

3.4. Remplacement de l'article 48 de la loi n° 78-17 pour introduire un mécanisme de retrait d'agrément

3.4.1. Option 1 (écartée) : Se limiter aux manquements des seuls responsables de traitement et sous-traitants

Les articles 45 et 46, tels que proposés par le projet de loi, prévoient des mesures correctrices à l'encontre des responsables de traitement et sous-traitants, ainsi que le garantit le règlement. Il aurait dès lors été possible de ne pas prévoir d'autres possibilités de mises en demeure ou sanction. Cette possibilité a été écartée.

3.4.2. Option 2 (retenue) : Prévoir un mécanisme de retrait d'agrément

Il apparaît nécessaire de prévoir des pouvoirs répressifs contre d'autres types d'opérateurs que le règlement place dans le champ de compétence de la Commission nationale de l'informatique et des libertés, à savoir les organismes de certification de l'article 43 du règlement et les organismes chargés du respect d'un code de conduite de l'article 41 de ce même règlement.

En effet, dans le cadre de la nouvelle logique de responsabilisation prévue par le règlement, ces opérateurs vont jouer un rôle important pour accompagner les responsables de traitement ou sous-traitants. Il est donc apparu pertinent de pouvoir prononcer à leur encontre un retrait d'agrément

[53] CE, 27 juillet 2012, AIS2, n° 340026.

lorsque ces derniers ont manqué à leur obligation ou n'ont pas respecté les dispositions de la loi ou du règlement.

Pour la procédure, il est renvoyé à celle applicable aux responsables de traitements pour souci de clarté.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

La présente disposition vise à remplacer et à adapter les articles 45 à 48 de la loi n° 78-17 pour conférer à la Commission nationale de l'informatique et des libertés de nouveaux pouvoirs. Certains d'entre eux ont un impact juridique direct dès lors que ces mesures, même si elles ne présentent pas toutes le caractère de sanction, constituent des décisions susceptibles de recours[54].

Le texte proposé permet une meilleure articulation avec les procédures de cohérence, de coopération et d'urgence prévues par le règlement.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

Dans la mesure où le règlement est construit sur une logique de renforcement du contrôle *a posteriori* des autorités de contrôle, accompagné d'un accroissement substantiel du montant des amendes, en contrepartie de l'allègement du contrôle *ex ante* du fait de la suppression de la plupart des formalités préalables pour les responsables de traitement, une augmentation des recours dirigés contre les décisions prises par la Commission nationale de l'informatique et des libertés au titre de sa mission de contrôle pourrait intervenir.

Toutefois, cette augmentation pourrait rester mesurée au vu du nombre de sanctions infligées par la CNIL en 2016 (13 sanctions, dont 4 sanctions financières et 9 avertissements).

4.3. IMPACTS SUR LES FINANCES PUBLIQUES

Les sanctions envisagées par le règlement étant plus proportionnées aux bénéfices des responsables de traitement, particulièrement les grands groupes multinationaux (jusqu'à 20 millions euros ou 4 % du chiffre d'affaires annuel, contre 3 millions d'euros actuellement) et les sous-traitants étant également passibles de certaines mesures correctrices, elles pourraient avoir un effet positif sur les finances publiques dans certains cas de non-respect du règlement, les sanctions pécuniaires étant recouvrées comme les créances de l'État étrangères à l'impôt et au domaine.

Il est précisé par ailleurs que le projet de loi, maintenant sur ce point l'article 45 de loi n° 78-17, exclut la possibilité de prononcer des sanctions pécuniaires dans le cas de traitements mis en œuvre par l'Etat.

[54] Voir par exemple CE, 5 septembre 2008, Société Directannonces, n° 319071, à propos d'une mise en demeure.

4.4. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les mesures proposées, qui renforcent les pouvoirs de sanction et les mesures correctrices que peut prendre la Commission nationale de l'informatique et des libertés, peuvent concerner les collectivités territoriales, en tant qu'elles sont responsables de traitement.

Il convient de relever à cet égard que les contrôles opérés concernent majoritairement les opérateurs de secteur privé. Ainsi, en 2016, comme l'année précédente, 70 % des missions de contrôle réalisées ont concerné le secteur privé, 30 % le secteur public. S'agissant plus spécifiquement des contrôles en ligne, ce sont 90 % des vérifications qui ont été menées dans le secteur privé[55].

Les sanctions prononcées par la Commission à l'encontre des collectivités territoriales restent également peu nombreuses : un seul avertissement non public à une collectivité territoriale (en raison de données inadéquates, non pertinentes et excessives et un défaut d'information concernant un traitement de gestion des inscriptions scolaires) et deux mises en demeure non publiques à des communes (pour défaut d'information des personnes et défaut de sécurité et de confidentialité en matière de demande d'état civil en ligne, et défaut d'information et d'accord préalable des personnes en matière de dépôt de cookies) en 2015[56]. En revanche, aucune sanction financière n'a été prononcée à l'encontre d'une collectivité territoriale en 2015 et en 2016.

4.5. IMPACTS SUR LES PARTICULIERS

L'impact des mesures proposées est très important puisqu'elles sont de nature à assurer une réelle effectivité des droits des personnes concernées par des mesures dissuasives et proportionnées. En particulier, l'astreinte envisagée assurera le caractère dissuasif des mesures correctrices dans le temps.

Enfin, la publication des mesures permettra une meilleure information des personnes concernées quant aux comportements relatifs à leurs données.

4.6. IMPACTS SUR LES ENTREPRISES

Les mesures proposées ont pour objet d'avoir un effet dissuasif sur les entreprises, responsables de traitement, mais également sous-traitants de ces derniers.

Dans le cas d'un avertissement, les entreprises qui seraient susceptibles de violer les dispositions pourraient éviter des amendes administratives importantes, lesquelles sont substantiellement renforcées par le règlement.

5. CONSULTATIONS ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

[55] Rapport d'activité 2016 de la Commission nationale de l'informatique et des libertés.
[56] Rapport d'activité 2015 de la Commission nationale de l'informatique et des libertés.

Le Conseil national d'évaluation des normes a également été consulté, en application de l'article L. 1212-2 du code général des collectivités territoriales, et a rendu un avis favorable lors de sa séance du 30 novembre 2017.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du projet de loi renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 6 (III)	Décret en Conseil d'Etat	Définition de la procédure d'urgence contradictoire.

CHAPITRE II

DISPOSITIONS RELATIVES A CERTAINES CATEGORIES DE DONNEES

ARTICLE 7

DONNEES SENSIBLES

1. DIAGNOSTIC

1.1. ETAT DES LIEUX

Le premier alinéa de l'article 8 de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, issu de la transposition de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, pose le principe de l'interdiction de collecter ou de traiter « *des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* ». Il s'agit de données qui touchent à l'intimité de la personne ou sont susceptibles de donner lieu à des discriminations.

Des dérogations à cette interdiction sont toutefois prévues, tenant soit à l'objet du traitement soit au consentement de l'intéressé, pour :

- Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée (consentement susceptible d'être affecté par un lien de subordination, une situation particulièrement éprouvante ou contrainte, etc.) ;

- Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;

- Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical, sous certaines conditions ; il s'agit du cas où la donnée constitue l'objet même de l'association ou de l'organisme avec lequel la personne entretient volontairement une relation ;

- Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;

- Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

- Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

- Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels ;

- Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé.

Deux autres dérogations sont également prévues : l'une fondée sur « l'anonymisation à bref délai », qui permet, dès lors que les conditions de sécurité sont remplies, de considérer le risque d'exploitation de la donnée sensible comme nul ; l'autre, tenant à « l'intérêt public » du traitement mis en cause, qui peut justifier la collecte et le traitement des données sensibles. Dans ce cas, les traitements doivent être autorisés par la Commission nationale de l'informatique et des libertés sur le fondement des articles 25 ou 26 de la loi n° 78-17 selon les cas de figure.

L'énumération actuelle des données dites « sensibles » à l'article 8 de la loi n° 78-17 ne correspond pas tout à fait aux catégories particulières de données à caractère personnel énoncées à l'article 9 du règlement (UE) 2016/679 ou à celles prévues à l'article 10 de la directive (UE) 2016/680.

Par rapport à la rédaction du premier alinéa de l'article 8 de la loi n° 78-17, les deux textes européens prévoient également, dans le champ des données sensibles, les données génétiques et les données biométriques. Ils contiennent par ailleurs des différences sémantiques : l'origine au singulier et non au pluriel, le terme de « convictions » religieuses ou philosophiques plutôt que celui d'« opinions ». Il en va, enfin de même concernant les données sur « la vie sexuelle ou l'orientation sexuelle », tandis que le droit national mentionne seulement la « vie sexuelle ».

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel, dans sa décision du 29 juillet 2004, se prononçant sur l'article 8 de la loi n° 78-17, a jugé que ces dispositions se bornent à tirer les conséquences nécessaires des dispositions inconditionnelles et précises du e) du 2 de l'article 8 de la directive 95/46/CE du 24 octobre 1995 sur lesquelles il ne lui appartient pas de se prononcer. Dès lors, et conformément à sa jurisprudence relative à la transposition des directives européenne, le Conseil a jugé conforme à la Constitution l'article 8 de la loi du 6 janvier 1978, après avoir considéré que le grief tiré de l'atteinte au respect de la vie privée, invoqué à l'encontre de la dérogation prévue à l'interdiction

de traitement de données sensibles pour les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice, ne peut être utilement présenté devant lui[57].

Il a confirmé sa jurisprudence à propos de la dérogation également prévues pour les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé[58].

1.3. CADRE CONVENTIONNEL

L'article 6 de la convention n° 108 du Conseil de l'Europe du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, prévoit que : *« Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales* ».

Le « paquet européen de protection des données » pose également, de façon similaire pour le règlement (UE) 2016/679 (article 9) et pour la directive UE 2016/680 (article 10), un principe d'interdiction de traitement des données sensibles, assorties de certaines exceptions: « *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. […]* ».

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

L'objectif poursuivi par cette disposition est la mise en cohérence de l'ensemble du droit national afin de proposer un cadre juridique unifié pour l'encadrement des traitements des données dites « sensibles ».

2.2. NECESSITE DE LEGIFERER

Il est nécessaire de modifier les dispositions de la loi n° 78-17 qui entrent dans le champ d'application du règlement général de protection des données et de la directive en ajoutant les données génétiques et les données biométriques aux fins d'identifier une personne physique de manière unique à cette liste. Ces données font déjà l'objet d'une protection particulière en droit national de par les formalités préalables qui leur est appliqué (régimes d'autorisation prévus aux articles 25 et 27 de la loi n° 78-17).

[57] Décision n°2004-499 DC du 29 juillet 2004.
[58] Décision n°2014-412 QPC du 19 septembre 2014.

Dans un souci de cohérence, il est proposé d'appliquer une énumération unique des données sensibles à l'ensemble du projet de loi.

3. OPTIONS

3.1. Option 1 (écartée) : Ne pas modifier l'énumération des catégories particulières de données pour les traitements qui ne relèvent pas du champ du droit de l'Union européenne

Il pourrait être envisagé de ne modifier la liste des catégories particulières de données que pour les traitements relevant de la directive. Le règlement étant d'application directe, cette définition trouvera à s'appliquer sans nécessité de modifier la loi n° 78-17 pour les traitements entrant dans le champ du règlement.

Ainsi, deux listes distinctes mais proches subsisteraient dans l'ordre juridique interne. Cela créerait une difficulté d'appréhension du droit par les acteurs d'une part, conduirait à une baisse du niveau de protection des données à caractère personnel les plus sensibles dans certains traitements mis en œuvre par l'Etat (défense nationale par exemple) et pour les données sensibles des personnes décédées, d'autre part.

Dans un souci de cohérence du droit de la protection des données à caractère personnel, cette option n'a pas été retenue.

3.2. Option 2 (retenue) : Définition unique des catégories particulières de données pour l'ensemble du droit national

Il est proposé d'augmenter le niveau de protection en intégrant dans le champ des données sensibles les données biométriques et génétiques pour l'ensemble du droit national, y compris pour les traitements ne relevant pas du droit de l'Union européenne.

En effet, la France a toujours protégé ces deux catégories particulières de données (notamment par la mise en place de la formalité préalable d'autorisation) même si elles n'apparaissaient pas dans la liste énoncée au premier alinéa de l'article 8 de la loi n° 78-17. Cette insertion permet d'interdire en principe leur traitement.

Dans un souci de cohérence du droit national, ainsi que de sécurité juridique tant pour les responsables de traitement que pour les personnes concernées, il est proposé d'étendre la qualification de catégorie particulière de données aux données génétiques et biométriques, à l'instar du droit européen applicable, à l'ensemble des dispositions nationales.

Dans la mesure où les données biométriques constituent des données sensibles dont le traitement est en principe interdit, il est apparu nécessaire de maintenir une dérogation à l'interdiction posée au premier alinéa de l'article 8 pour les traitements mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques nécessaires aux contrôles de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions

confiées aux salariés ou aux agents, actuellement autorisés par la CNIL[59] sur le fondement de l'article 25 de la loi n° 78-17 abrogé par le présent projet de loi.

La dérogation également prévue pour les traitements mis en œuvre par l'Etat, dans l'exercice de ses prérogatives de puissance publique, portant sur des données génétiques ou biométrique aux fins d'authentification ou d'identification, est quant à elle maintenue (cf. infra, article 9).

Ces dérogations complètent les cas dans lesquels des données sensibles peuvent être exceptionnellement traitées en vertu du deuxième alinéa de l'article 8 de la loi n° 78-17, outre les cas prévus par l'article 9.2 du règlement.

Enfin, la loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté a remplacé dans le code pénal et d'autres textes l'expression « en raison de la race » par « en raison de la prétendue race ». Il est apparu cohérent de faire de même pour la notion « d'origine raciale », et de parler de « prétendue origine raciale » dans le cadre de la loi n°78-17[60].

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGÉE

4.1. IMPACTS JURIDIQUES

L'impact juridique est l'insertion de deux nouvelles catégories particulières de données dont le traitement est en principe interdit : les données génétiques et les données biométriques aux fins d'identifier une personne physique de manière unique.
Les modifications sémantiques sont quant à elles mineures et ne devraient pas emporter d'impact juridique par rapport au droit existant. En effet, et à titre d'exemple, si l'article 8 de la loi n° 78-17, dans sa rédaction actuelle, ne mentionne pas expressément l'orientation sexuelle parmi les données sensibles, le juge fait déjà une interprétation extensive des données relatives à la vie sexuelle pour y intégrer cette notion. Ainsi, le Conseil d'Etat a jugé que les données relatives aux signataires de pacte civil de solidarité, si elles n'ont pas pour objet de révéler les orientations sexuelles des personnes concernées, peuvent néanmoins permettre de déduire l'existence d'une vie de couple entre des personnes de même sexe, ce qui justifie la limitation à certaines catégories de tiers de la communication de ces informations[61].

4.2. IMPACTS SUR LES PARTICULIERS

Du fait de l'interdiction de principe de traiter ces catégories particulières de données, le droit à la protection des données à caractère personnel est renforcé à l'égard des personnes concernées pour les traitements ne relevant pas du droit de l'Union européenne.

[59] Délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052).
[60] Les termes de « prétendue race » qui avaient été critiqués devant le Conseil constitutionnel, ont été déclarés conformes à la Constitution (décision n° 2016-745 DC du 26 janvier 2017).
[61] CE, 8 décembre 2000, Conseil supérieur et l'administration de biens et a., n° 217046 et 217826.

5. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

TITRE II

MARGES DE MANOEUVRE PERMISES PAR LE REGLEMENT (UE) 2016/679 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIF A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES, ET ABROGEANT LA DIRECTIVE 95/46/CE

CHAPITRE I^{ER}

CHAMP D'APPLICATION TERRITORIAL DES DISPOSITIONS COMPLETANT LE REGLEMENT (UE) 2016/679

ARTICLE 8

CRITERE D'APPLICATION DU DROIT

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La question du champ d'application du règlement (UE) 2016/679 constitue l'une des innovations majeures par rapport à la directive 95/46/CE. L'article 3 du règlement prévoit un double champ d'application.

D'une part, il est applicable aux traitements effectués dans le cadre des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant dès lors que celui-ci se trouve sur le territoire de l'Union, peu importe que le traitement ait lieu ou non dans l'Union. Il s'agit en quelque sorte d'un critère organique (article 3-1).

D'autre part, le règlement est également applicable selon un « critère matériel », peu important que l'établissement soit sur le territoire de l'Union, dès lors que le traitement est effectué à l'égard des résidents européens. Il suffit alors que l'offre de biens ou de services à des personnes concernées se déroule dans l'Union ou que leur comportement dans l'Union soit suivi (article 3-2).

Le règlement a donc une cohérence globale vis-à-vis des responsables de traitements présents dans ou en dehors de l'Union. Il précise à cet égard qu'il « *devrait s'appliquer aux personnes*

physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données ».

Si le champ d'application du règlement (UE) 2016/679 est déjà défini par celui-ci, en revanche, le champ d'application des marges de manœuvres des États membres octroyées par le règlement doit être défini afin d'éviter des conflits de normes en cas de dispositions divergentes selon les législations nationales.

En effet, se pose la question du critère à retenir pour la législation applicable entre États membres de l'Union en cas de divergences compte tenu des choix différents dans l'exercice des marges de manœuvre permises par le règlement. Cette question n'est pas abordée par ce dernier. Les spécificités nationales peuvent concerner les droits de la personne concernée, le responsable du traitement et le sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, la coopération et la cohérence, ainsi que les situations particulières de traitement des données.

Par exemple, l'article 9(4) du règlement permet une marge de manœuvre plus protectrice en ce qui concerne les traitements de données génétiques, biométriques ou concernant la santé. Si la France est plus protectrice qu'un autre Etat membre, se posera la question du droit applicable au traitement réalisé dans cet autre Etat membre et relatif à un résident en France.

Cette question pose des enjeux en termes de protection des droits fondamentaux des personnes concernées (par exemple s'agissant de l'âge du consentement des mineurs), mais également d'attractivité du territoire dès lors que la législation applicable peut constituer un critère important pour une entreprise qui souhaite s'implanter à l'étranger.

Actuellement, l'article 5 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit le champ d'application suivant :

« I. - Sont soumis à la présente loi les traitements de données à caractère personnel :
1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;
2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.

II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui. »

En vertu de cet article, le droit national s'applique lorsque le responsable est établi en France (I-1°) ou à défaut, en absence d'établissement en France ou dans l'Union européenne, lorsque le responsable recourt à des moyens de traitement sur le territoire français (I-2°). Ces critères de

détermination du droit applicable ne tiennent pas compte du lieu de résidence de la personne concernée.

L'article 8 du présent projet de loi doit se lire en cohérence avec l'article 3 du règlement précité, directement applicable à compter du 25 mai 2018.

L'article propose ensuite, pour l'application des marges de manœuvres ainsi que les autres dispositions, de retenir le critère de résidence de la personne concernée, à l'exception des traitements mentionnés à l'article 85-2 du règlement, en matière de la liberté d'expression et d'information qui relèveraient du critère d'établissement du responsable de traitement.

1.2. CADRE CONVENTIONNEL

Le règlement a une cohérence globale vis-à-vis des responsables de traitements présents dans ou en dehors de l'Union. Il précise à cet égard qu'il « *devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données* » (considérant 14).

En ce qui concerne les marges de manœuvre, le règlement est en revanche silencieux, à l'exception de son considérant 153 qui indique, s'agissant des exemptions au nom de la liberté d'expression et d'information (article 85), que *« Dans le cadre du traitement de données à caractère personnel uniquement à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré par l'article 11 de la Charte. Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse. / (…) Lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme. ».* L'article 85.1 du règlement, en écho à ce considérant, prévoit que les Etats membres peuvent prévoir des exemptions ou dérogations si elles sont nécessaires pour concilier le droit la protection des données et la liberté d'expression et d'information.

C'est la raison pour laquelle le projet de loi réserve en particulier cette situation qui trouvera à s'appliquer par exemple dans le domaine de la presse.

1.3. ELEMENTS DE DROIT COMPARE

Lors des réunions relatives à la mise en œuvre du règlement qui ont eu lieu à la Commission européenne, sont apparues des positions divergentes entre les Etats membres. Certains ont annoncé qu'ils retiendraient un critère d'établissement unique pour l'ensemble des marges de manœuvres, d'autres semblent privilégier des critères combinant l'établissement et la résidence. Enfin, certains Etat préfèrent ne pas inscrire de critères dans leur projet de loi afin de laisser les règles classiques de conflits de normes s'appliquer.

Par exemple, la loi allemande (section 1 (4))[62] semble privilégier formellement un critère d'établissement qui ne serait pas nécessairement celui de l'établissement principal. Outre la situation des organismes publics, la loi allemande est applicable pour les organismes privés si :

- le responsable de traitement ou le sous-traitant traite des données personnelles en Allemagne ;

- les données à caractère personnel sont traitées dans le contexte d'une activité d'un établissement en Allemagne ;

- si le responsable de traitement ou le sous-traitant, bien que n'ayant pas d'établissement dans un Etat membre, relève du champ d'application du règlement.

Or l'article 4 du règlement définit le « traitement » comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

Par conséquent, dès lors qu'un responsable de traitement traite une donnée d'une personne présente en Allemagne (y compris la collecte) alors le droit allemand s'appliquera, ce qui revient à appliquer un critère semblable à celui proposé par le projet de loi.

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

La précision dans la loi du critère d'application a pour objet de garantir une sécurité juridique pour les responsables de traitement afin de connaître quelle est la législation applicable en cas de législation différente entre Etats membres de l'Union européenne. Une telle sécurité juridique participe de l'attractivité du territoire national.

[62] « This Act shall apply to public bodies. It shall apply to private bodies if: 1. the controller or processor processes personal data in Germany, 2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany, or if, 3. although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it does fall within the scope of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4 May 2016, p. 1; L 314 of 22 November 2016, p. 72).
If this Act does not apply in accordance with the second sentence, only Sections 8 to 21 and 39 to 44 shall apply to the controller or processor. »

Il s'agit également de garantir la protection des données à caractère personnel des personnes présentes sur le territoire français.

2.2. NECESSITE DE LEGIFERER

Le règlement ne contient aucune disposition relative aux critères d'applicabilité du droit lorsque des règles nationales précisant des marges de manœuvre permises par le règlement conduisent à des divergences de législation entre Etats membres de l'Union européenne.

Dans ces conditions, la loi nationale pourrait être silencieuse, laissant le soin aux tribunaux d'appliquer le droit applicable en cas de contentieux. Toutefois, cette option ne semble pas satisfaisante au regard, d'une part, du principe de sécurité juridique, d'autre part, des enjeux liés aux droits des personnes concernées.

3. OPTIONS

3.1. Inscrire dans la loi un critère d'application

3.1.1. Option 1 (écartée) : Ne rien prévoir dans la loi

Il aurait pu être décidé de ne rien indiquer dans la loi et laisser les juridictions, en cas de contentieux, appliquer les règles classiques en cas de conflit de normes internationales. Cette option ne semblait pas satisfaisante au regard des objectifs de sécurité juridique, ce d'autant que le règlement ne contient aucune disposition sur ce point.

3.1.2. Option 2 (retenue) : Fixer dans la loi des critères d'application

Par souci de sécurité juridique, il a été préféré de prévoir expressément dans la loi les critères d'application en cas de divergences de législations entre Etats membres liées aux marges de manœuvre prévues par le règlement.

A titre d'exemple, s'agissant de la marge de manœuvre permise par l'article 8 du règlement relatif à l'âge du consentement des enfants en ce qui concerne les services de la société de l'information, l'article 3 alinéa 3 du code civil dispose que : « *Les lois concernant l'état et la capacité des personnes régissent les Français, même résidant en pays étranger* ».

La définition de la majorité, et corrélativement de la minorité, est indubitablement à rattacher à la capacité des personnes. La détermination des actes susceptibles d'être réalisés, par exception, par le mineur semble devoir l'être également. En effet, dans le code civil, l'article 388-2 par exemple relève du titre X relatif à la minorité, la tutelle et l'émancipation, et non du titre IX relatif à l'autorité parentale, bien que l'intervention des administrateurs légaux soit nécessaire. Le critère d'application du droit français fondé sur la nationalité de l'article 3 alinéa 3 du code civil est donc actuellement applicable.

Si l'on souhaite qu'un autre critère lui soit substitué pour la question de la capacité du consentement d'un mineur au traitement des données personnelles, en l'occurrence le critère de la

résidence, une disposition légale spécifique est nécessaire pour déroger à ce principe, comme par exemple l'article 311-14 du code civil pour la loi applicable à la filiation.

3.2. Choix du critère d'application

3.2.1. Option 1 (écartée) : critère de l'établissement du responsable de traitement

Les principes du marché intérieur du droit de l'Union européenne conduiraient à privilégier le critère de l'établissement principal du responsable du traitement, c'est-à-dire le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement ait le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal.

Le critère d'établissement aurait pour avantage premier de permettre au responsable de traitement de n'appliquer qu'un seul droit. Cela permet de réduire les charges administratives et la complexité juridique pour ce responsable.

Dans une telle hypothèse, le droit applicable aux personnes concernées pourrait varier en fonction du lieu d'établissement principal du responsable de traitement ou de son sous-traitant.

Cela reviendrait à faire application du droit d'autres Etats membres pour des traitements de données qui touchent des résidents français. Par exemple, si l'Irlande choisit, comme âge de consentement des mineurs en ce qui concerne l'offre directe de services de la société de l'information, l'âge de 13 ans, cette disposition s'appliquerait aux résidents français pour ce qui est de l'utilisation de services tels que Google ou Facebook dont le siège de leur filiale européenne se trouve en Irlande.

3.2.2. Option 3 (retenue) : Lieu de résidence de la personne concernée

Le critère du lieu de la collecte de la donnée est opportun lorsqu'il est préférable d'appliquer le régime national à des domaines spécifiques, notamment lorsque ce droit est plus protecteur.

Ce critère est plus protecteur pour les personnes physiques concernées, qui n'ont alors pas à s'interroger sur le droit applicable dans un autre Etat membre de l'Union, lequel n'est bien souvent pas accessible dans leur langue. Le considérant 14 du règlement précise à cet égard que : « *La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel.* »

En outre, une telle option est plus respectueuse de la souveraineté du droit national : dès lors qu'il s'agit d'une marge de manœuvre, les États membres appliquent leur droit lorsqu'il s'agit d'adapter ou de compléter les droits et obligations prévus par le règlement.

Dans le cas où une autorité de contrôle d'un autre Etat membre de l'Union serait autorité de contrôle chef de file (logique de « guichet unique »), celle-ci serait tenue d'appliquer le droit français s'il s'agit de constater un manquement pour un résident. Le juge du pays de l'autorité de

contrôle concernée pourrait ainsi potentiellement se prononcer sur l'application et l'interprétation du droit français.

Dès lors que les Etats membres ne se sont pas entendus sur certaines dispositions et que des marges de manœuvre existent, il est cohérent que chaque Etat puisse appliquer les choix politiques que le législateur national a faits.

3.3. Exclusion pour les traitements relatifs à la liberté d'expression et d'information

3.3.1. Option 1 (écartée) : Aucune dérogation

Il aurait pu être proposé de ne prévoir aucune dérogation pour ce type de traitement, ce qui aurait conduit à faire application du critère du lieu de résidence de la personne comme pour les autres marges de manœuvre.

Cette option a été écartée pour deux raisons.

D'une part, le considérant 153 du règlement précise que *« lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer »*.

D'autre part, en matière de traitements à des fins journalistiques, il est important que le droit applicable soit celui du lieu d'établissement eu égard aux exigences liées à la liberté de la presse et des médias. Ainsi, une entreprise de presse établie en France n'aura pas à respecter des prescriptions particulières d'un autre Etat membre lorsqu'elle traite des données à caractère personnel.

3.3.2. Option 2 (retenue) : Prévoir une dérogation pour les traitements relatifs à la liberté d'expression et d'information

Prenant en compte le considérant 153 du règlement, le projet de loi prévoit une dérogation au critère de résidence au droit applicable qui dépendra du lieu de l'établissement.

Cette hypothèse a vocation à concerner par exemple les traitements de données à caractère personnel à des fins de journalisme et leur cession à des fins commerciales. A cet titre, la Cour de justice a jugé que : *« L'article 9 de la directive 95/46 doit être interprété en ce sens que les activités mentionnées à la première question, sous a) à d), concernant des données provenant de documents publics selon la législation nationale, doivent être considérées comme des activités de traitement de données à caractère personnel exercées "aux seules fins de journalisme" au sens de cette disposition, si lesdites activités ont pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées, ce qu'il appartient à la juridiction nationale d'apprécier »*[63].

[63] CJUE, 16 décembre 2008, l'affaire C-73/07.

Ainsi, par exemple, un site internet de presse établi en France n'aura pas à respecter des prescriptions particulières d'un autre Etat membre lorsqu'elle traite des données à caractère personnel. Dans le cadre d'une procédure de coopération engagée dans le cadre d'un traitement transfrontalier à l'égard d'un responsable de traitement établi en France, c'est le droit national qui s'appliquerait, notamment s'agissant des pouvoirs de la CNIL. Ainsi, le responsable de traitement pourrait opposer le secret des sources journalistiques qui s'appliquera en France (comme le prévoit l'article 4 du projet de loi), ce qui ne serait pas forcément le cas dans un autre Etat membre de l'Union européenne, l'article 90 du règlement permettant à chaque Etat membre d'adopter des règles spécifiques en matière d'obligations de secret.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

La disposition proposée permet de garantir une plus grande sécurité et une meilleure accessibilité juridique, tant pour les entreprises et les particuliers, qui connaîtront le critère permettant de définir le droit applicable en cas de législations nationales divergentes au sein de l'Union européenne, que pour les juridictions, appelées à trancher un conflit de normes qui pourrait se présenter dans le cadre de recours dont elles seraient saisies.

4.2. IMPACTS SUR LES PARTICULIERS

La disposition proposée vise à assurer une protection plus importante des droits des personnes concernées lorsque le législateur ou le pouvoir règlementaire décide de mettre en œuvre une marge de manœuvre.

4.3. IMPACT SUR LES ENTREPRISES

Pour les responsables de traitement et sous-traitants ayant un établissement en France, cette mesure n'a aucun impact.

Pour les autres responsables de traitement ayant un établissement à l'étranger (sur le territoire de l'Union européenne ou à l'extérieur), il leur appartiendra de respecter les dispositions de la loi française lorsque celle-ci aura prévu d'adapter ou de compléter les droits et obligations prévus par le règlement.

5. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

CHAPITRE II

DISPOSITIONS RELATIVES A LA SIMPLIFICATION DES FORMALITES PREALABLES A LA MISE EN OEUVRE DES TRAITEMENTS

ARTICLE 9

ALLEGEMENT DES FORMALITES PREALABLES

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés consacre un chapitre aux formalités préalables à la mise en œuvre des traitements (Chapitre IV, articles 22 à 31) qui donne un rôle central à la Commission nationale de l'informatique et des libertés.

Pour être mis en œuvre, les traitements doivent soit être déclarés à la Commission nationale de l'informatique et des libertés (article 22) soit autorisés par celle-ci (article 25) soit encore autorisés par arrêté ou décret en Conseil d'Etat après avis de la Commission (article 26 et 27).

Cette gradation dans les formalités préalables tient compte à la fois de la finalité du traitement, de sa sensibilité en termes de type de données traitées et de l'identité de son responsable.

Exemples de traitements soumis aux formalités prévues par les articles 25 à 27 de la loi n° 78-17 :

Loi n° 78-17 actuelle	Exemples
Article 25	
I. - Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :	
1° Les traitements, automatisés ou non, mentionnés au 7° du II [statistiques INSEE], au III [données rapidement anonymisées] et au IV [intérêt public] de l'article 8 ;	- Délibération n° 2008-005 du 10 janvier 2008 portant autorisation unique de mise en œuvre par les entreprises ou organismes exploitants de médicaments de traitements automatisés de données à caractère personnel relatifs à la gestion des données de santé recueillies dans le cadre de la

	pharmacovigilance des médicaments postérieurement à leur mise sur le marché (n° AU-013) [article 8.IV] ; - Délibération n° 2013-406 du 19 décembre 2013 autorisant le ministère de l'intérieur à mettre en œuvre un dispositif composé de deux traitements automatisés de données à caractère personnel ayant pour finalités la gestion des candidatures ainsi que le suivi des mandats électoraux et des fonctions électives. [article 8.IV].
2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;	- Délibération n° 2006-131 du 9 mai 2006 portant autorisation de mise en œuvre par l'unité 525 de l'Institut national de la santé et de la recherche médicale INSERM) d'une banque d'ADN et d'ARN de patients présentant une athérosclérose coronarienne ; - Délibération n° 2015-090 du 12 mars 2015 autorisant le laboratoire TOXGEN à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des données administratives et techniques relatives à l'établissement d'empreintes génétiques dans le cadre des expertises judiciaires. (Combinaison du 25-I-2° et 3°) ; - Délibération n° 2017-252 du 14 septembre 2017 autorisant le Centre national de la recherche scientifique à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude de la diversité génétique et linguistique de la population du Cap-Vert (Demande d'autorisation n° 1972648).
3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;	- Délibération n°2004-095 du 09 décembre 2004 portant autorisation d'un traitement automatisé de données à caractère personnel présenté par le vice-président du Conseil d'État et concernant la gestion des activités contentieuses du Conseil d'Etat, des cours administratives d'appel et des tribunaux administratifs ; - Délibération n° 2008-491 du 11 décembre 2008 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion précontentieuse des infractions constatées par les commerçants sur les lieux de vente (décision d'autorisation unique n° AU-016) ;

	- Délibération n° 2016-036 du 11 février 2016 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion du contentieux lié au recouvrement des contraventions au code de la route et à l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au code de la route, abrogeant la délibération n° 2006-188 du 6 juillet 2006 (décision d'autorisation unique n° AU-010).
4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;	- Délibération n°2008-008 du 22 janvier 2008 autorisant la mise en œuvre par la Ville de Paris et par la Société des Mobiliers Urbains pour la Publicité et l'Information (SOMUPI) d'un traitement de données à caractère personnel ayant pour finalité la gestion de fichier de personnes à risque dans le cadre du système de location de vélos Vélib' (autorisations n°1247032 et n° 1247035) **;** - Délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit ; **-** Délibération n° 2009-359 du 18 juin 2009 portant autorisation unique des traitements automatisés de détection des alertes d'abus de marché mise en œuvre par les organismes du groupe Caisse d'épargne (demande d'autorisation n° 1232905) ; - Délibération n° 2009-422 du 2 juillet 2009 autorisant la mise en œuvre au sein du groupe Crédit agricole d'un traitement automatisé de données à caractère personnel ayant pour finalité la préqualification et l'aide à la décision en matière d'octroi de crédit aux professionnels (autorisation n° 1291301) ; - Délibération n° 2009-429 du 2 juillet 2009 portant autorisation unique des traitements de données à caractère personnel mis en œuvre par les sociétés du Groupe des assurances du Crédit mutuel dont la finalité est la lutte contre le blanchiment de capitaux et le financement du terrorisme (demande d'autorisation n° 1360717) ; - Délibération n° 2014-012 du 16 janvier 2014 autorisant la mise en œuvre par la Banque Populaire Rives de Paris d'un traitement visant la lutte contre la fraude interne.

5° Les traitements automatisés ayant pour objet : - l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ; - l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;	- Délibération n° 2011-083 du 17 mars 2011 portant autorisation unique de traitements de données à caractère personnel aux fins d'exercice des activités notariales et de rédaction des documents des offices notariaux ; - Délibération n° 2014-526 du 11 décembre 2014 autorisant la mise en œuvre par le Pari Mutuel Urbain (PMU) d'une interconnexion entre ses fichiers ressources humaines et clients afin de lutter contre les conflits d'intérêt.
6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;	- Délibération n° 2008-579 du 18 décembre 2008 autorisant l'Association pour la gestion des informations sur le risque en assurance (AGIRA) à traiter les données à caractère personnel relatives aux décès transmises par l'INSEE et portant autorisation unique des traitements automatisés des entreprises d'assurances, des institutions de prévoyance et de leurs unions, et des mutuelles et de leurs unions mis en œuvre aux fins de recherche des assurés et des bénéficiaires de contrats d'assurance sur la vie décédés ; - Délibération n° 2016-096 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de la prévention et de la protection de l'enfance (AU-49) (Combinaisons des articles 8 (IV), 9 (1°), 25 (I, 1°), 25 (I, 3°), 25 (I, 6°) et 25 (I, 7°)) ; - Délibération n° 2017-174 du 1er juin 2017 autorisant l'association départementale les pupilles de l'enseignement public de la Vienne à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité l'accompagnement et le suivi social et médico-social des personnes handicapées(Demande d'autorisation n° 1920331) (25-I-6° et 7°).
7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;	- Délibération n°2008-181 du 26 juin 2008 portant autorisation de mise en œuvre par le Ministère du logement et de la ville et par le Ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire de deux traitements de données à caractère personnel dénommés « DALO » et « DALORIF » ; - Délibération n°2011-225 du 21 juillet 2011 autorisant l'association La Rose des Vents à mettre

	en œuvre le traitement des demandes d'hébergement d'urgence et de logement d'insertion.
8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;	- Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail ; - Délibération n° 2017-251 du 14 septembre 2017 autorisant la Société Générale à mettre en œuvre un système d'identification par reconnaissance faciale des prospects lors d'une entrée en relation à distance.
9° Par dérogation au 1° du I et aux 1° et 2° du II de l'article 27, les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de recherche scientifique ou historique, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code spécifique non signifiant, propre à chaque projet de recherche, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique. L'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu ne peuvent être assurés par la même personne ni par le responsable de traitement. L'opération cryptographique est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis motivé et publié de la	- Délibération n° 2016-372 du 1er décembre 2016 portant avis sur un projet de décret en Conseil d'Etat portant application des dispositions du I bis de l'article 22 et 9° du I de l'article 25 de la loi du 6 janvier 1978. Il s'agit du décret 2016-1930 du 28 décembre 2016 portant simplification des formalités préalables relatives à des traitements à finalité statistique ou de recherche.

Commission nationale de l'informatique et des libertés.	
II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.	- Délibération n° 2008-007 du 10 janvier 2008 portant autorisation unique de traitements de données à caractère personnel aux fins d'exercice des activités notariales et de rédaction des documents des offices notariaux ; - Délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.
Article 26	
I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :	
1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;	- Arrêté du 15 avril 2009 portant création d'un traitement de données à caractère personnel relatif à la délivrance d'habilitations, d'agréments et au suivi de la validité des titres de circulation des personnes exerçant une activité dans les zones d'accès restreint des ports maritimes dénommé « CEZAR (Contrôle d'entrée en zone d'accès restreint) » ; - Arrêté du 19 mars 2012 portant création d'un traitement de données à caractère personnel relatif au suivi du trafic maritime dénommé « TRAFIC 2000 ».
2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. L'avis de la commission est publié avec l'arrêté autorisant le traitement.	- Arrêté du 16 janvier 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « numérisation des procédures pénales » ; - Arrêté du 10 décembre 2008 portant création par le ministère de l'intérieur d'un traitement automatisé de données à caractère personnel dénommé « base satellite VV » [relatif au vol et à la mise sous surveillance d'un véhicule] ; - Arrêté du 22 décembre 2008 portant création d'un traitement automatisé dénommé « GARDIAN »

	relatif au suivi de la gestion des biens saisis placés en gardiennage.
II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.	- Décret n°97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie et modifiant le code de la sécurité sociale et le code de la santé publique (deuxième partie : Décrets en Conseil d'Etat).
III. - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.	- Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (en son article 2 : fichiers non publiés).
IV. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.	- Arrêté du 2 mars 2007 portant création, à titre expérimental, d'un traitement automatisé de contrôle des données signalétiques des véhicules ; - Arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules ; - Arrêté du 14 avril 2009 autorisant la mise en œuvre de traitements automatisés dans les communes ayant pour objet la recherche et la constatation des infractions pénales par leurs fonctionnaires et agents habilités.
Article 27	
I.- Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :	
1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles	- Décret n° 2015-691 du 18 juin 2015 autorisant le traitement automatisé de données à caractère personnel dénommé « Piper » (production d'informations sur les personnels relevant du ministère de la défense) ; - Décret n° 2009-1300 du 26 octobre 2009 autorisant la création d'un traitement automatisé de gestion des personnels des cultes d'Alsace et de Moselle ; - Décret n° 2017-665 du 27 avril 2017 relatif au

figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;	traitement de données à caractère personnel de gestion des conditions matérielles d'accueil des demandeurs d'asile, dénommé DNA ; - Décret n° 2009-1310 du 26 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour géré par l'Office français de l'immigration et de l'intégration.
2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.	- Décret n° 2013-147 du 18 février 2013 relatif à l'application de gestion des dossiers de ressortissants étrangers en France et au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa ; - Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (TES) ; - Décret n° 2017-880 du 9 mai 2017 autorisant les traitements de données à caractère personnel destinés à la mise en œuvre de l'allocation personnalisée d'autonomie et de l'aide sociale à l'hébergement.
II.- Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :	- Décision du Conseil général des Alpes-Maritimes relative à la mise en œuvre d'un traitement de données à caractère personnel ayant pour finalité de contrôler le revenu de solidarité active ; - Arrêté du 25 septembre 2008 relatif à la mise en service à la direction générale des finances publiques, à la Caisse nationale des allocations familiales et à la Caisse centrale de mutualité sociale agricole d'une procédure automatisée de transfert des données fiscales.

1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ; 2° Sous réserve du 9° du I de l'article 25, ceux des traitements mentionnés au I : -qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ; -qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ; -et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques.	- Arrêté du 6 février 2009 portant création d'un traitement de données à caractère personnel dénommé « Répertoire partagé des professionnels de santé » (RPPS).
3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;	- Arrêté du 9 juillet 2009 portant création d'un traitement automatisé réalisé à l'occasion du recensement de la population de Nouvelle-Calédonie en 2009 ; - Arrêté du 20 août 2009 modifiant l'arrêté du 19 juillet 2000 portant création d'un traitement automatisé d'informations individuelles relatif à la constitution et à la mise à jour par l'INSEE du répertoire d'immeubles localisés (RIL) ; - Arrêté du 23 mars 2010 modifiant l'arrêté du 12 janvier 2004 autorisant la mise en œuvre des phases « saisie et exploitation des données collectées » et « contrôle de la cohérence des réponses aux enquêtes » du traitement « Recensement de la population ».
4° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de	- Arrêté du 22 mai 2017 portant création d'un traitement de données à caractère personnel dénommé « Réexamen élevage IED » ; - Arrêté du 16 juin 2017 autorisant la mise en œuvre

l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.	d'un traitement automatisé de données à caractère personnel dénommé « Trouver mon master ».

En 2016, la Commission nationale de l'informatique et des libertés a reçu 102 629 dossiers de formalités, dont 54 000 dossiers de formalités simplifiées. Elle a accordé 190 autorisations et a reçu 316 demandes d'autorisation en matière de biométrie[64].

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel s'est prononcé sur le numéro d'inscription des personnes au répertoire national d'identification (NIR) dans une décision du 29 décembre 1998[65], à propos des traitements de données relatifs à l'assiette, au contrôle et au recouvrement de tous impôts, droits, taxes, redevances ou amendes de façon interconnectée entre trois directions du ministère de l'économie et des finances.

Il a écarté le grief tiré de la méconnaissance des exigences constitutionnelles relatives à la protection de la vie privée et de la liberté individuelle, en estimant que l'utilisation du numéro d'inscription au répertoire national d'immatriculation des personnes physiques a pour finalité d'éviter les erreurs d'identité, lors de la mise en œuvre des traitements de données en vigueur, et ne conduit pas à la constitution de fichiers nominatifs sans rapport direct avec les opérations incombant aux administrations fiscales et sociales.

1.3. CADRE CONVENTIONNEL

Le règlement (UE) 2016/679 introduit en droit de la protection des données le principe de responsabilisation (« *accountability* » en anglais). L'article 5(2) du règlement indique ainsi que : « *le responsable du traitement est responsable du respect du paragraphe 1[des principes relatifs au traitement des données à caractère personnel] et est en mesure de démontrer que celui-ci est respecté (responsabilité)* ».

[64] Rapport d'activité 2016 de la Commission nationale de l'informatique et des libertés.
[65] Décision n° 98-405 DC du 29 décembre 1998

La logique de la responsabilisation est décrite à l'article 24(1) du règlement qui prévoit que : « *Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.* ».

La responsabilité peut également comprendre la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

L'ajout du principe de responsabilisation parmi les principes relatifs au traitement des données à caractère personnel a une incidence importante sur la pratique des responsables de traitements et des sous-traitants. Suivant la logique nouvelle de responsabilisation qu'il introduit, le règlement induit une réduction importante des formalités préalables pour la mise en œuvre de traitements ayant pour contrepartie un renforcement des pouvoirs des autorités de contrôle et du montant des sanctions pécuniaires qu'elles peuvent infliger aux responsables de traitement et sous-traitants (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'entreprise).

En d'autres termes, il s'agit du passage d'une logique de déclaration *ex ante* auprès d'une autorité nationale de protection des données à une logique de responsabilisation des organismes traitant des données qui doivent assurer la protection de telles données dès la conception des outils, réaliser des études d'impact préalables et mettre en place des mécanismes de certification.

Le responsable du traitement et le sous-traitant auront l'obligation de tenir une documentation, en particulier un registre des activités de traitement (article 30 du règlement).

Le règlement maintient toutefois des formalités pour certains types de traitements : analyse d'impact en cas de risque élevé (article 35), consultation préalable de l'autorité de contrôle (article 36) et, le cas échéant, autorisation de celle-ci (article 36(5)) en cas de risque résiduel élevé pour la protection des données.

La Commission nationale de l'informatique et des libertés a publié une méthode pour les analyses d'impacts[66]. Le G29, groupe de travail regroupant l'ensemble des autorités de contrôle des Etats de l'Union européenne, a également publié des lignes directrices sur le sujet[67].

Enfin, le règlement prévoit la possibilité de maintenir des régimes nationaux plus stricts pour certaines catégories de données : « conditions supplémentaires » pour les données génétiques, biométriques et de santé (art. 9.4) ; « garanties appropriées » pour les données d'infractions (art. 10) ; régime d'« autorisation préalable » pour les traitements effectuées dans le cadre d'une « mission d'intérêt public […] y compris le traitement dans le cadre de la protection sociale et de la santé publique » (art. 36-5) ; « règles plus spécifiques » pour les relations de travail (art. 86),

[66] https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil

[67] Voir Groupe de travail « Article 29 » sur la protection des données, « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation» http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083,

« conditions spécifiques » pour le traitement du numéro d'identification national (art. 87). 2. Objectifs et necessite de legiferer

2.1. OBJECTIFS POURSUIVIS

La modification du régime des formalités préalables prévue par le projet de loi vise à respecter la nouvelle logique du règlement, dans le contexte d'une unification du cadre juridique au sein de l'Union européen, afin d'éviter les écueils du « forum shopping » des entreprises.

Elle répond ainsi à un objectif de simplification administrative pour les entreprises en termes d'allègement des formalités préalables, tout en renforçant la responsabilisation des organismes traitant des données, ainsi que de leurs sous-traitants.

2.2. NECESSITE DE LEGIFERER

Compte tenu de la logique générale du règlement basée sur une responsabilisation des responsables de traitement et un maintien de garanties en cas de risque élevé pour la protection des données (exigence d'analyse d'impact relative à la protection des données), il apparaît nécessaire de revoir l'ensemble du régime d'autorisation prévu actuellement par la loi n° 78-17, tout en préservant certaines garanties pour des traitements particulièrement sensibles.

En effet, certaines formalités préalables ne respectent ni le texte ni l'esprit du règlement. Le projet de loi doit simplifier les régimes existants en ne laissant subsister que ce qui est couvert par le règlement et nécessité par la nature sensible du traitement.

Il convient ainsi de s'en tenir au « risque élevé » comme critère d'une saisine préalable de la Commission nationale de l'informatique et des libertés. Sauf exception, ce risque devra être apprécié, selon la logique de responsabilisation qui est celle du règlement, par le responsable de traitement et non par matière.

Il est précisé que les traitements relevant de l'article 26 de loi n° 78-17 ne sont pas concernés par les modifications induites par le règlement. Ainsi, demeureront autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

3. OPTIONS

3.1. Suppression du régime déclaratoire de l'article 22

3.1.1. Option 1 (écartée) : Maintien d'un tel régime

Ce régime déclaratif qui constitue actuellement la formalité préalable de droit commun, n'apparait plus compatible avec le règlement.

En outre, ainsi qu'a pu le souligner le rapport du Conseil d'Etat sur le numérique et les droits fondamentaux, ce système déclaratif s'expose à différents reproches :

« *Il conduit à transmettre à la CNIL une masse considérable d'informations, d'inégal intérêt en raison des enjeux très variables pour la protection des données personnelles. Si l'obligation de déclaration est assez simple à respecter pour des entreprises ne mettant en œuvre que des traitements courants (par exemple, un fichier du personnel et un fichier des clients), elle peut s'avérer plus lourde pour des acteurs, notamment ceux de l'économie numérique, qui ont une activité intense et évolutive de traitement des données. Les « startups», en particulier, sont susceptibles de voir évoluer au cours de leurs premières années leur modèle d'affaires et, corrélativement, leurs modalités d'utilisation des données personnelles ; en raison de leur petite taille, elles peuvent avoir plus de difficulté à appréhender leurs obligations de déclaration et sont ainsi exposées à une certaine insécurité juridique. Pour autant, l'obligation de déclaration ne met pas à disposition de la CNIL toutes les informations nécessaires pour évaluer le degré de sensibilité d'un traitement ; en particulier, la CNIL n'est informée ni du nombre de personnes dont les données sont traitées, ni du volume des données transmises à des tiers* »[68].

3.1.2. Option 2 (écartée) : Passage d'un régime de déclaration à celui d'une autorisation de certains traitements

Il aurait pu être envisagé que certains traitements contenant le numéro d'inscription des personnes au répertoire national d'identification (NIR) et soumis actuellement à un régime de déclaration soient basculés dans un régime plus contraignant, à savoir celui de la consultation préalable obligatoire de l'autorité de contrôle.

Cette option est contraire à la logique du règlement.

3.1.3. Option 3 (retenue) : Remplacement des dispositions relatives à la déclaration et abrogation des articles 23 et 24 de la loi de 1978

Le projet de loi abroge le régime déclaratif prévu aux articles 22 à 24 de la loi n° 78-17. Par mesure de lisibilité, l'article 9 du projet de loi rappelle le principe de la consultation préalable qui existe dans le règlement : « *Conformément à l'article 36 du règlement (UE) 2016/679, le responsable du traitement consulte la Commission nationale de l'informatique et des libertés préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données*

[68] Conseil d'Etat, Etude annuelle 2014, *« Le numérique et les droits fondamentaux »*, la documentation française, p.177

effectuée au titre de l'article 35 dudit règlement indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ».

Il est en effet important de rappeler cette notion de « risque élevé » d'autant que le projet de loi supprime les autorisations de l'article 25 et la plupart de celles de l'article 27 de la loi n° 78-17 (cf. infra mesure 3.2).

3.2. Suppression des régimes d'autorisation

L'article 25 de la loi n°78-17 prévoit des autorisations préalables de la Commission nationale de l'informatique et des libertés, à l'exclusion des traitements mentionnés aux articles 26 et 27.

3.2.1. Option 1 (écartée) : Maintenir en l'état l'ensemble des régimes d'autorisation

Le règlement ne prévoit pas de possibilité pour les Etats membres de conserver un régime d'autorisation, sauf dans l'hypothèse de l'article 36.5 du règlement ou au titre des conditions supplémentaires pour les données sensibles (art. 9), des garanties complémentaires pour les données d'infraction (art. 10) et des conditions spécifiques du traitement du numéro d'identification national (article 87).

Cette option consistant au maintien d'un régime général d'autorisation auprès de la Commission nationale de l'informatique et des libertés n'a donc pas été retenue.

3.2.2. Option 2 (retenue) : Suppression de la plupart des autorisations (articles 25 et 27)

Le règlement n'oblige pas d'abroger l'ensemble des régimes d'autorisation existants. Le projet de loi épouse la logique du règlement en évitant des obligations supplémentaires inutiles. Toutefois, au regard de l'enjeu de la protection des données, le projet de loi conserve un régime d'autorisation préalable pour deux types de données.

En premier lieu, les traitements mis en œuvre pour le compte de l'Etat qui portent sur des génétiques, ou des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes conservent un régime d'autorisation par décret après avis de la Commission nationale de l'informatique et des libertés.

En effet, les données génétiques constituent des données sensibles en vertu de l'article 9 du règlement. Il s'agit de données « relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » (art. 4 du règlement).

De telles données peuvent indiquer des prédispositions génétiques concernant des individus et à ce que ces données peuvent être utilisées pour d'autres finalités. Ce type de données ne relève pas uniquement des traitements dans le domaine de la santé (test génétique) qui fait l'objet d'un régime particulier (nouveau chapitre IX), mais peut également être utilisées à des fins

d'identification d'une personne (empreintes génétiques), de son ascendance ou descendance (test de paternité) ou de recherche scientifique (étude génétique de populations)[69].

De même, la donnée biométrique n'est pas une donnée d'identité comme les autres : elle n'est pas attribuée par un tiers ou choisie par la personne, mais elle est produite par le corps lui-même et le désigne de façon définitive (caractère non révocable). Dans ces conditions, confier ses données biométriques à un tiers n'est pas un acte anodin. La Commission nationale de l'informatique et des libertés est à cet égard très vigilante sur les risques liés à l'usage de la biométrie, en particulier dans le cadre des technologies biométriques « à traces » telles que l'empreinte digitale, dont l'usage, en cas de conservation dans une base centralisée, peut être détourné : usurpation d'identité, violation des données, détournement de leur finalité[70]. Ce risque est d'autant plus important en cas d'interconnexion de fichiers : compte tenu de l'interopérabilité croissante des technologies d'identification biométrique, le stockage centralisé des données biométriques augmente le risque que des données biométriques soient utilisées pour relier différentes base entre elles[71].

Toutefois, le projet de loi prévoit de maintenir le régime d'autorisation à l'égard de ce type de traitement, uniquement lorsqu'ils sont mis en œuvre par l'Etat agissant dans l'exercice de ses prérogatives de puissance publique. Lorsque l'Etat agit comme toute autre personne ou organisme (contrôle d'accès aux locaux de ses services par exemple, comme le ferait tout employeur ou toute entreprise), une autorisation par décret en Conseil d'Etat ne serait plus exigée.

En second lieu, les traitements qui mettent en œuvre le Numéro d'Inscription au Répertoire (NIR) par des personnes publiques ou privées, conservent une formalité préalable.

En effet, le NIR constitue un numéro particulièrement signifiant en ce qu'il comporte 13 caractères permettant de déterminer le sexe, l'année et le mois de naissance, et dans la majorité des cas, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger et enfin le numéro d'ordre qui permet de distinguer les personnes nées au même lieu à la même période. Il s'agit d'un numéro unique et pérenne, qui est susceptible de faire l'objet d'interconnexion dans différents fichiers sociaux, fiscaux…. De très nombreux traitements d'organismes de sécurité sociale (DSS, CNAMTS, CNAV, MDPH…) mais également d'autres organismes utilisent le NIR ainsi que des acteurs privés pour la gestion de la paie, des déclarations sociales, des déclarations d'embauche.

La CNIL contrôle de manière très stricte la pertinence de l'utilisation du NIR. A titre d'exemple, la commission a refusé la création d'un traitement par une société financière spécialisée dans le

[69] Les traitements concernant des données génétiques mis en œuvre par l'Etat dans le cadre de fichiers de souveraineté (ex : Fichier national automatisé des empreintes génétiques - FNAEG) continueront à relever du régime d'autorisation prévu à l'article 26. Lorsque les données génétiques sont traitées en tant que données se rapportant à la santé des personnes, les dispositions du chapitre IX s'appliqueront.

[70] Voir *Informatique et libertés, Le droit de la protection des données à caractère personnel en droit français et européen*, Anne Debet, Nathalie Metallinos et Jean Massot, Lextenso, 2015.

[71] Voir par exemple, à propos du fichier TES (titres électroniques sécurisés), créé par le décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

crédit à la consommation qui souhaitait utiliser le NIR à des fins de détection d'incohérences dans les demandes de crédit[72] (en l'espèce, la société souhaitait pouvoir identifier les fausses fiches de paie en généralisant automatiquement le numéro de sécurité sociale à partir des données de d'état civil connues du demandeur de crédit et en comparant de manière automatisée le numéro ainsi généré avec celui figurant sur les feuilles de paie).

Le projet de loi prévoit toutefois un allègement des formalités liées à la mise en œuvre de traitements mettant en œuvre le NIR. Il propose ainsi de prévoir un décret cadre, pris après avis motivé et publié de la commission, pour autoriser l'utilisation du NIR par catégorie de responsables de traitement et pour des finalités précises, dans la même logique que ce prévoyait la loi n° 78-17[73], avant sa modification par la loi n° 2004-801 du 6 août 2004[74].

Cette procédure d'autorisation de traitements utilisant le NIR ne sera pas applicable aux traitements bénéficiant d'ores et déjà d'une absence de formalité ou de formalités allégées[75] dès lors que le numéro d'inscription au répertoire national d'identification des personnes physiques fait l'objet préalablement d'une opération cryptographique lui substituant un code statistique non signifiant. Il s'agit des traitements qui ont exclusivement des finalités de statistique publique, de recherche scientifique ou historique ou qui mettent à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique.

Le régime de décret-cadre sera en revanche applicable aux traitements portant sur les alertes sanitaires lorsqu'ils portent sur NIR (cf. infra,).

En dernier lieu, les autres autorisations prévues aux articles 25 et 27 de la loi n° 78-17 sont abrogées. Ces traitements seront soumis au droit commun prévu par le règlement, à savoir, une consultation de la CNIL préalablement au traitement lorsqu'une analyse d'impact révèle que le traitement présenterait un risque élevé si le responsable ne prend pas les mesures pour atténuer ce risque(article 36).

3.3. Dispositions relatives à l'analyse d'impact

3.3.1. Option 1 (écartée) : Apporter une précision

L'article 35 du règlement est d'application directe. Par conséquent le responsable du traitement effectue préalablement à la mise en œuvre du traitement, une analyse d'impact relative à la protection des données. Toutefois, le 10 de l'article 35 du règlement prévoit une marge de manœuvre qu'il serait possible de réserver.

---

[72] Délibération portant refus d'autorisation de mise en œuvre par la société VOLKSWAGEN FINANCES d'un traitement automatisé de données à caractère personnel ayant pour finalité l'utilisation du numéro de sécurité sociale à des fins de détection d'incohérence dans les demandes de crédit

73 L'ancien article 18 de la loi n° 78-17 (avant 2004) disposait que : « *l'utilisation du répertoire national d'identification des personnes physiques en vue d'effectuer des traitements nominatifs est autorisée par décret en Conseil d'État pris après avis de la commission* »

[74] Voir pour un exemple pris sous l'empire de la loi avant 2004, Décret n° 91-1404 du 27 décembre 1991 autorisant l'utilisation du NIR par les employeurs pour les traitements de gestion de la paie et de la gestion du personnel,

[75] Articles 22 I bis et V, 27 II 4° de la loi n°78-17.

En effet, lorsque le traitement effectué « *est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis* »- ou *à « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »*, a une base juridique nationale, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 (de l'article 35) ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

Il serait possible de renvoyer à un décret en Conseil d'Etat après avis de la Commission nationale de l'informatique et des libertés pour préciser la liste des traitements spécifiques et ensembles d'opérations de traitement pour lesquels une analyse d'impact est obligatoire.

Or ce renvoi ne semble ni obligatoire ni utile. Par ailleurs, il ne semble pas possible de prévoir en amont cette liste de traitements spécifiques.

3.3.2. Option 2 (retenue) : Ne rien mentionner

Le mécanisme mis en place par l'article 35.10 du règlement semble être le suivant : soit la norme qui met en place un traitement effectué en application des articles 6(1) c) et e) n'a pas fait l'objet d'une analyse d'impact, alors une telle analyse d'impact sera obligatoire avant les activités de traitement ; soit la norme a fait l'objet d'une telle analyse d'impact et par principe, les traitements ne sont pas soumis à une telle analyse sauf – et c'est là la marge de manœuvre – le droit de l'Etat membre l'indique de façon précise pour tel ou tel traitement.

Il semble plus pertinent, dans la logique du règlement (UE) 2016/679, de prévoir que c'est lorsque la norme règlemente le traitement que le législateur ou le pouvoir règlementaire doit s'interroger sur la nécessité ou non de prévoir une nouvelle analyse d'impact.

Par conséquent, la modification de la loi n° 78-17 ne semble pas être l'option pertinente[76].

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

Si le projet de loi supprime la plupart des formalités préalables lorsque les traitements relèvent du champ d'application du règlement (UE) 2016/679, il crée un régime d'autorisation allégé en ce qui concerne les traitements utilisant le Numéro d'Inscription au Répertoire (NIR).

[76] Une circulaire pourra appeler une attention particulière sur la protection des données à caractère personnel et la nécessité de prévoir une analyse d'impact au sens du règlement. Voir en ce sens, la circulaire n° 5598/SG du Premier ministre du 23 août 2012 relative à la prise en compte dans la préparation des textes législatifs et réglementaires de leur impact en termes d'égalité entre les hommes et les femmes définit des orientations particulières en termes de prise en compte, dans les travaux d'évaluation préalable, de la dimension des droits des femmes et de l'égalité entre les hommes et les femmes. Egalement, la circulaire n° 5602/SG du Premier ministre du 4 septembre 2012 relative à la prise en compte du handicap dans les projets de loi précise les modalités d'évaluation préalable portant sur la nécessité d'introduire dans le projet de loi des dispositions adaptées à la situation des personnes handicapées.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

L'allégement des formalités préalables est de nature à réduire le risque contentieux lié au refus d'autorisation de traitement de données par la Commission nationale de l'informatique et des libertés. L'impact pour les services judiciaires devrait toutefois être minime dans la mesure où le nombre de contentieux en la matière est marginal (à titre d'exemple, la Commission a opposé 9 refus à des demandes d'autorisation en matière de biométrie sur les 316 demandes reçues en 2016).

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales traitent chaque jour de nombreuses données à caractère personnel, que ce soit pour assurer la gestion administrative de leur structure (fichiers de ressources humaines), la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance) ou la gestion des différents services publics et activités dont elles ont la charge.

Les collectivités territoriales sont également concernées par l'allègement des formalités préalables, s'agissant en particulier de la suppression des déclarations auprès de la Commission nationale de l'informatique et des libertés et du régime d'autorisation par arrêté des traitements destinés à mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, ou de l'assouplissement du régime d'autorisation des traitements utilisant le Numéro d'Inscription au Répertoire (NIR) par un décret-cadre.

En tant que responsables de traitement, les collectivités territoriales sont toutefois soumises à l'obligation de tenir un registre des activités de traitement effectuées sous leur responsabilité. A l'instar des petites et moyennes entreprises (cf. infra), le règlement tient compte toutefois de la situation des petites collectivités territoriales en prévoyant que sont dispensées d'une telle obligation les organisations comptant moins de 250 employés, sauf si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte sur des données sensibles (article 30.5).

4.4. IMPACT SUR LES ENTREPRISES

Actuellement, le régime déclaratif présente une certaine lourdeur : la déclaration doit obligatoirement comporter les informations qui conditionnent l'appréciation de la licéité du traitement, notamment l'identité du responsable de traitement, la finalité du traitement, les données collectées, les destinataires, les éventuels transferts des données vers des pays non membres de l'Union européenne et la durée de conservation.

En outre, dans la mesure où la déclaration constitue une formalité préalable obligatoire, cela emporte des conséquences juridiques importantes. Ainsi, dès lors qu'un fichier client informatisé, n'ayant pas été déclaré, n'est pas dans le commerce, sa vente à un tiers a un objet illicite[77] .

Le projet de loi allège les formalités préalables auxquelles sont actuellement soumises les entreprises lorsqu'elles souhaitent mettre en œuvre un traitement.

[77] Cour de cassation, Com. 25 juin 2013, n°12-17.037.

Le responsable de traitement n'a plus d'obligation de déclarer les traitements qu'il souhaite mettre en œuvre ou solliciter l'autorisation préalable de la Commission nationale de l'informatique et des libertés, sauf en cas de risque élevé.

En revanche, les entreprises, en tant que responsables de traitement ou sous-traitants, resteront soumises aux obligations prévues par le règlement (tenue d'un registre d'activités des traitements[78], conduite d'une analyse d'impact,…). La situation des petites et moyennes entreprises est toutefois prise en compte. Ainsi, le considérant 13 du règlement précise que : « *Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte une dérogation pour les organisations occupant moins de 250 employés en ce qui concerne la tenue de registres. Les institutions et organes de l'Union, et les États membres et leurs autorités de contrôle sont en outre encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement.* »[79].

En cas de non-respect des obligations prévues par le règlement ou la loi, les entreprises s'exposent à des amendes pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (20 millions d'euros ou 4% du chiffre d'affaires en cas de réitération du manquement[80].

Selon le syndicat professionnel du numérique (Syntec Numérique), les projets de mise en conformité au règlement européen sur la protection des données vont tirer le secteur de l'édition logicielle et du conseil informatique. Ce syndicat anticipe en 2018 une croissance du chiffre d'affaires du secteur de 3,6%, par rapport à 2017, en partie liée aux budgets engagés par leurs clients pour préparer leur mise en conformité au règlement[81].

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Le Conseil national d'évaluation des normes a également été consulté, en application de l'article L. 1212-2 du code général des collectivités territoriales et a rendu un avis favorable lors de sa séance du 30 novembre 2017.

[78] Art. 30.5 du règlement (UE) 2016/679.
[79] Article 30.5 du règlement : « *5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10* ».
[80] Art. 83 du règlement.
[81] Les Echos, 7 décembre 2017.

5.2. MODALITES D'APPLICATION

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du projet de loi renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 9 (I, 2° alinéa)	Décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés	Détermination des catégories de responsables de traitement et des finalités des traitements au vu desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le NIR
Article 9 (I, 7° alinéa	Décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés	Détermination de la fréquence de l'opération cryptographique substituant un code statistique non signifiant au NIR

CHAPITRE III

OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENTS ET SOUS-TRAITANTS

ARTICLE 10

SOUS-TRAITANT

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

Le chapitre V de la loi du 6 janvier 1978 décrit les obligations qui incombent aux responsables de traitements (article 32 à 37), au-delà du simple respect des droits des personnes concernées consacrées dans le même chapitre (articles 38 à 43*ter*). Les obligations incombant aux responsables de traitement sont détaillées dans une première section.

Les obligations incombant au sous-traitant, généralement le prestataire technique en charge de la mise en œuvre technique du traitement de données, sont précisées à l'article 35 de la loi n° 78-17[82]. En vertu de cet article, le sous-traitant est regardé comme étant celui qui traite des données à caractère personnel pour le compte du responsable de traitement (article 3). La principale obligation du sous-traitant, au-delà de ses engagements contractuels, est le respect des conditions de sécurité, posées par l'article 34, sans pour autant que cela décharge le responsable de traitement de sa responsabilité d'y veiller. Les autres obligations pèsent, en droit, sur le responsable de traitement, à charge pour celui-ci d'exiger le respect des garanties posées par la loi par son sous-traitant dans un cadre contractuel.

L'émergence de nouveaux outils numériques, à l'instar du *cloud computing*, a conduit cependant la Commission européenne comme les autorités de contrôle européennes, chacune en ce qui la concerne, à s'interroger sur les obligations particulières des sous-traitants.

Le règlement (UE) 2016/679 et la directive (UE) 2016/680 qui renforcent les obligations pensant sur les responsables de traitement dans le cadre de la logique de responsabilisation, ont étendu le champ de ces obligations au sous-traitant défini comme « *la personne physique ou morale,*

[82] *« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. / Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. / Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. / Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »*

l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[83].

A cet égard, le considérant 81 du règlement précise que : « *Afin que les exigences du présent règlement soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce dernier confie des activités de traitement à un sous-traitant, le responsable du traitement ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement.* »

1.2. CADRE CONVENTIONNEL

Le règlement (UE) 2016/679 et la directive (UE) 2016/680 renforcent la responsabilisation des responsables de traitement ainsi que des sous-traitants. Le chapitre IV du règlement (UE) 2016/679 précise les obligations des responsables de traitement et sous-traitants. L'article 28 du règlement (UE) 2016/679 précise les principales obligations applicables spécifiquement au sous-traitant.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Le projet de loi a pour objectif de clarifier la distinction entre les dispositions d'application de la directive (UE) 2016/680 et les obligations directement applicables du règlement (UE) 2016/680 à la charge des sous-traitants.

En complétant l'article 35 de la loi n° 78-17 par une référence aux obligations prévues par le chapitre IV du règlement (UE) 2016/679 pour les sous-traitants intervenant dans le cadre de traitement relevant de ce règlement, la disposition répond également à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi[84].

2.2. NECESSITE DE LEGIFERER

La disposition proposée résulte d'une nécessité de clarification afin de préciser l'articulation des dispositions nationales de transposition de la directive (UE) 2016/680 (article 22 du projet de loi) avec les obligations du règlement (UE) 2016/680.

[83] Article 4 – 8) du règlement (UE) 2016/679, article 3-9) de la directive (UE) 2016/680.
[84] Décision n° 2005-514 DC du 28 avril 2005, cons. 14

3. OPTIONS

3.1.1. Option 1 (écartée) : Maintenir uniquement les dispositions de transposition

Il aurait pu être envisagé que seules les dispositions de transposition de la directive (UE) 2016/680 soient présentes dans la loi (article 19 du projet de loi).

Le texte aurait manqué de lisibilité pour les personnes concernées et organismes quant aux obligations des sous-traitants.

3.1.2. Option 2 (écartée) : Etendre les obligations prévues par le règlement aux sous-traitants agissant dans le cadre de traitement relevant de la directive

Il aurait pu être envisagé d'appliquer les mêmes obligations aux sous-traitants dans le champ de la directive (UE) 2016/680. Toutefois, la directive (UE) 2016/680 impose une transposition qui prévoit d'autres obligations.

Cette option a donc été écartée, un article spécifique introduit par l'article 19 du projet de loi (article 70-10) précisant le régime applicable aux sous-traitants dans le cadre des traitements relevant de la directive.

3.1.3. Option 2 (retenue) : Faire une simple référence aux obligations du règlement qui s'imposent aux sous-traitants pour les traitements relevant de celui-ci

Par souci de lisibilité, le projet de loi rappelle, à l'article 35 de la loi n° 78-17 que dans le champ d'application du règlement (UE) 2016/679, le sous-traitant respecte les conditions prévues au chapitre IV de ce règlement.

Pour les traitements ne relevant ni du règlement, ni de la directive, les dispositions de l'actuel article 35 de la loi n°78-17 trouveront à s'appliquer.

Il est enfin précisé que les mesures correctrices et sanctions susceptibles d'être prises par la CNIL en vertu de l'article 6 du projet de loi ont vocation à s'appliquer également aux sous-traitants, quel que soit le champ d'application dont relève le traitement dont ils assurent la prestation.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGÉE

4.1. IMPACTS JURIDIQUES

La disposition précise l'articulation entre les dispositions de la loi n° 78-17 et le règlement (UE) 2016/679 concernant le régime de la sous-traitance des responsables de traitement.

4.2. IMPACTS SUR LES PARTICULIERS

Les dispositions proposées assurent une meilleure lisibilité et permettent donc aux particuliers de mieux connaitre les obligations des organismes traitant leurs données à caractère personnel lorsque ces derniers ont recours à des prestataires extérieurs.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les dispositions proposées assurent une meilleure lisibilité et permettent donc aux collectivités territoriales de mieux comprendre les obligations qui pèsent sur les sous-traitants auxquels elles peuvent avoir recours dans le cadre de la mise en œuvre de traitement.

4.4. IMPACT SUR LES ENTREPRISES

Les dispositions proposées assurent une meilleure lisibilité et permettent donc aux entreprises de mieux comprendre leurs obligations en tant que sous-traitant d'un responsable de traitement.

Les entreprises, en tant que responsable de traitement, lorsqu'elles auront recours à un prestataire, devront respecter les dispositions de l'article 28 du règlement.

5. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Le Conseil national d'évaluation des normes a été consulté et a rendu un avis favorable sur ce projet de texte lors de sa séance du 30 novembre 2017.

CHAPITRE IV

DISPOSITIONS RELATIVES A CERTAINES CATEGORIES PARTICULIERES DE TRAITEMENT

ARTICLE 11

DONNEES D'INFRACTION

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

L'article 9 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés constitue, avec l'article 8, le cadre qui régit le traitement des données intrinsèquement sensibles, lesquelles ne peuvent être collectées que dans des conditions particulières.

Cet article concerne les données d'infractions, condamnations et mesures de sûreté. Ces données peuvent en effet emporter de graves conséquences si elles sont révélées à autrui, notamment lorsqu'elles sont conservées au-delà des durées de prescription légale.

Le traitement de telles données est doublement encadré :

- d'une part, en termes de formalités préalables, de tels traitements étant actuellement soumis au régime d'autorisation prévu par l'article 25-3° de la loi n° 78-17 ;
- d'autre part, le nombre limité de responsables qui peuvent mettre en œuvre ces traitements.

Ainsi, outre les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales, peuvent également mettre en œuvre de tels traitement, les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi et, depuis la loi n° 2004-801 du 6 août 2004, les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle dans le cadre de la lutte contre les atteintes à la propriété littéraire et artistique

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel a analysé les dispositions de la loi n° 78-17 sur les traitements relatifs aux données d'infraction dans sa décision du 29 juillet 2004[85].

[85] Décision n°2004-499 DC du 29 juillet 2004.

A cette occasion, le Conseil constitutionnel a précisé que les garanties appropriées et spécifiques en raison de l'ampleur que pourraient revêtir les traitements de données à caractère personnel relatifs à des données d'infractions, eu égard à l'atteinte éventuel au droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, doivent être fixées dans la loi (considérant 11). Les modalités d'application des exceptions au principe que seule l'autorité publique peut mettre en œuvre de tels traitements doivent aussi apparaître dans la même loi, et ne pas être renvoyées ou à du droit souple ou à des lois ultérieures (considérant 12).

Le projet de loi prévoit ainsi de réaffirmer l'interdiction de principe, commandée par le règlement, et de cibler les personnes qui, peuvent mettre en place ces traitements, sur certaines conditions et pour une finalité précise.

Dans sa décision du 29 juillet 2004, le Conseil constitutionnel a par ailleurs censuré les dispositions du 3° de l'article 9 de la loi n° 78-17[86] qui prévoyaient la possibilité accordée à une personne morale de droit privé, mandatée par plusieurs autres personnes morales victimes d'agissements pénalement sanctionnés – ou estimant en avoir été victimes ou pensant être susceptibles d'en être victimes – pour les besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi de rassembler un grand nombre d'informations nominatives relatives à des infractions, condamnations et mesures de sûreté, en raison de l'absence de garanties appropriées et spécifiques[87]. Le Conseil constitutionnel a en effet considéré que, compte tenu du champ, très large, couvert par une telle faculté, il appartenait au législateur de fixer les conditions dans lesquelles elle pouvait être exercée, sans pouvoir renvoyer à des lois ordinaires ultérieures.

---

[86] *« Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi. »*

[87] « *11. Considérant que le 3° de l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déférée, permettrait à une personne morale de droit privé, mandatée par plusieurs autres personnes morales estimant avoir été victimes ou être susceptibles d'être victimes d'agissements passibles de sanctions pénales, de rassembler un grand nombre d'informations nominatives portant sur des infractions, condamnations et mesures de sûreté ; qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en œuvre et de la nature des informations traitées, le 3° du nouvel article 9 de la loi du 6 janvier 1978 pourrait affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution ;*

12. Considérant que, s'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions ; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de « fraude » ; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations ; qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures ; que, par suite, le 3° du nouvel article 9 de la loi du 6 janvier 1978 est entaché d'incompétence négative ; »

Le Conseil a également formulé une réserve d'interprétation de l'article 9, tel que résultant de la déclaration d'inconstitutionnalité de son 3°. Pour le Conseil constitutionnel, cet article ne saurait être interprété comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime, afin de ne pas priver de base légale les traitements légitimement mis en œuvre par chaque personne morale pour suivre les dossiers contentieux relatifs aux infractions dont elle a été elle-même victime.

Le projet de loi, tenant compte de la censure du Conseil constitutionnel et de la réserve d'interprétation associée à sa décision, propose de permettre aux personnes physiques ou morales de pouvoir mettre en œuvre des traitements de données d'infraction afin de leur permettre de préparer et le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée proportionnée à cette finalité.

1.3. CADRE CONVENTIONNEL

Les traitements de données de nature pénale sont régis par la directive (UE) 2016/680 du 27 avril 2016 lorsqu'elles sont traitées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection la protection contre les menaces à la sécurité publique et la prévention de telles menaces. Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive (considérant 11 de la directive).

Le règlement (UE) 2016/679 s'applique en revanche lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins que celles prévues par la directive et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques et conformément au droit des États membres (considérant 11 de la directive).

De même, les États membres peuvent confier aux autorités compétentes d'autres missions qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de sorte que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du règlement (UE) 2016/679.

Le règlement prévoit d'ailleurs une disposition spécifique pour les données relatives aux condamnations pénales, aux infractions et aux mesures de sûreté connexes dont leur traitement, compte tenu de la nature de ces données, est strictement encadré.

L'article 10 du règlement prévoit ainsi que : *« Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes (…),*

ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. ».

Enfin, l'article 86 du règlement prévoit que : « *Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou au droit de l'État membre auquel est soumis l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du présent règlement.* ».

Cet article autorise ainsi le droit national à prévoir la réutilisation des données publiques contenues dans les décisions de justice, dans le respect du droit à la protection des données, ainsi que le prévoit l'article 11 du projet de loi.

1.4. ELEMENTS DE DROIT COMPARE

Dans son projet de loi organique, l'Espagne prévoit que les traitements de données de nature pénale à d'autres finalités que pénales ne pourront être mis en œuvre que sur la base d'une disposition au moins de rang législatif, d'une disposition de cette même loi organique ou soit sur la base d'un texte de l'Union européenne.

L'Irlande a prévu d'autres possibilités de traitements des données à caractère personnel relatives aux condamnations pénales et aux infractions que les seuls cas visés par le règlement (UE) 2016/679. A l'instar du présent projet de loi, l'Irlande a fait le choix d'utiliser la marge de manœuvre de l'article 11 du règlement, en ouvrant cette possibilité à 9 catégories de traitements[88].

Le projet de loi britannique prévoit 7 catégories de traitements possibles. Par exemple, les organisations non-lucratives à finalité politique, philosophique, religieuse ou syndicale, pourront sous certaines conditions, traiter des données de nature pénale de leurs membres ou anciens membres.

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Les modifications proposées à l'article 9 de la loi n° 78-17 par le projet de loi poursuivent plusieurs objectifs :

- un objectif de clarté et d'intelligibilité du droit en s'alignant sur la rédaction de l'article 9 de la loi n°78-17 sur celle prévue par l'article 10 du règlement (UE) 2016/679 ;

88

http://www.justice.ie/en/JELR/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf/Files/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf

- un renforcement de la protection des droits fondamentaux dès lors que le champ des données de données de nature pénale encadré par la loi est élargi, en couvrant par exemple les mesures de sûreté connexes ;
- un objectif de sécurité juridique, en permettant à des personnes qui ont une nécessité particulière de traiter des données de nature pénale de pouvoir le faire, dans un cadre strict afin que l'atteinte aux droits fondamentaux ne soit pas excessive ;
- une conciliation de la protection des données à caractère personnel avec la transparence de la justice, et le droit d'accès à l'information.

2.2. NECESSITE DE LEGIFERER

Si l'article 10 du règlement (UE) 2016/679 est directement applicable en droit national, il est nécessaire d'harmoniser les écritures dans un objectif de clarté et intelligibilité du droit. Pour cette raison, le premier alinéa de l'article 9 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés doit être modifié pour épouser la rédaction du règlement. Les données d'infractions sont entendues au sens large, incluant les mesures de sûreté connexes. L'insertion du critère « sous le contrôle de l'autorité publique », en plus de « mis en œuvre par » vise les traitements mis en œuvre pour le compte de l'autorité publique comme l'hébergement des données sur un serveur.

Le projet de loi prévoit également d'élargir le champ des personnes susceptibles de mettre en œuvre de tels traitements dans le cadre notamment du suivi des dossiers contentieux relatifs aux infractions, afin de tenir compte de la censure du Conseil constitutionnel dans sa décision du 29 juillet 2004.

En effet, actuellement, de nombreux traitements[89] ont été autorisés par la Commission nationale de l'informatique et des libertés en s'appuyant sur la réserve d'interprétation formulée par le Conseil constitutionnel dans sa décision du 29 juillet 2004. La Commission est d'ailleurs régulièrement saisie de demandes d'autorisation pour des fichiers « contentieux » ou « précontentieux » par des organismes privés ou publics, parmi lesquels figurent des infractions et des condamnations pénales.

Par conséquent, une réécriture du troisième paragraphe de l'article 9 de la loi n° 78-17 apparaît nécessaire en termes de sécurité juridique.

Enfin, il est apparu nécessaire, suite à l'adoption de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique qui permet désormais la mise à disposition du public à titre gratuit (*open data*) des décisions de justice, d'encadrer la réutilisation des données publiques de nature pénale contenues dans ces décisions.

[89] Les traitements portent sur des infractions constatées par les commerçants sur les lieux de vente par exemple, l'autorisation AU-017), la lutte contre la contrefaçon (par exemple, la délibération CNIL n°2011-111), incivilités des clients à l'égard des salariés (par exemple, la délibération CNIL n°2013-036), la gestion des procédures de conciliation (par exemple, la délibération CNIL n°2012-168).

3. OPTIONS

3.1. Elargissement du champ des personnes concourant au service public de la justice autorisées à mettre en œuvre des traitements de donnes d'infraction

3.1.1. Option 1 (écartée) : Maintien du droit existant

La rédaction actuelle du 1° l'article 9 de la loi n° 78-17 qui limite le champ d'application aux personnes seules personnes publiques et personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales, ne permet pas de prendre en compte les besoins d'autres personnes morales qui, sans avoir cette qualité, concourent au service public de la justice.

La rédaction actuelle du 1° de l'article 9 de la loi n° 78-17 apparaît par conséquent trop restrictive.

3.1.2. Option 2 (écartée) : Etendre à l'ensemble des personne concourant à un service public

Cette option consistant à donner la possibilité de mettre en œuvre de traitement des traitements de données d'infraction à l'ensemble des personnes morales « concourant à un service public » est apparue excessive eu égard à la sensibilité des données concernées.

Pour cette raison, cette option n'a pas été retenue.

3.1.3. Option 3 (retenue) : Limiter l'extension aux seules personnes morales de droit privé collaborant au service public de la justice

L'ajout proposé permet à des acteurs limités, dans un cadre circonscrit notamment en termes de finalité, de traiter des données de nature pénale, en tenant compte de la réserve d'interprétation formulée par le Conseil constitutionnel.

Il s'agit de maintenir l'interdiction de principe mais de permettre des personnes morales de droit privé (associations par exemple) œuvrant à partir de données d'infractions dans une mission de service public de la justice de mener à bien leur mission principale ou conformément à leur objet social.

Cette disposition vise notamment les associations d'aide aux victimes[90], ou les associations d'aide à la réinsertion des personnes placées sous main de justice[91]. L'impossibilité actuelle pour de tels acteurs qui ne gèrent pas un service public mais collaborent à celui-ci, de traiter des données de nature pénale nécessaire à leur activité nuit à la réalisation de leur mission.

---

[90] Actuellement, 166 associations d'aide aux victimes sont subventionnées par le programme 101 « Accès au droit et à la justice ».

[91] Article 3 de la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire : « *Le service public pénitentiaire est assuré par l'administration pénitentiaire sous l'autorité du garde des sceaux, ministre de la justice, avec le concours des autres services de l'Etat, des collectivités territoriales, des associations et d'autres personnes publiques ou privées.* »

3.2. Possibilité pour les personnes physiques ou morales de mettre en œuvre de tels traitements dans le cadre d'une action en justice en tant que victime

3.2.1. Option 1 (écartée) : Maintien du droit existant

Ainsi qu'il a été dit précédemment, plusieurs traitements autorisés par la Commission nationale de l'informatique et des libertés trouvent leur base légale sur la seule réserve d'interprétation du Conseil constitutionnel dans sa décision du 29 juillet 2004, aux termes de laquelle l'article 9 de la loi n° 78-17 « *ne saurait être interprété comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime*».

Cette situation n'est pas satisfaisante au regard du principe de sécurité juridique. Il appartient en effet au législateur de préciser davantage les conditions dans lesquelles un traitement de données d'infraction peut être mise en œuvre par une personne physique ou morale pour assurer sa défense en qualité de victime.

3.2.2. Option 2 (retenue) : Prévoir un encadrement des traitements relatifs à la gestion du contentieux par des personnes privées

Afin de répondre à un réel besoin tant pratique (la Commission est régulièrement saisie de demandes d'autorisation pour des fichiers « contentieux » ou « précontentieux » par des organismes privés) qu'en termes de sécurité juridique, il est proposé de rétablir le 3° de l'article 9 de la loi n° 78-17 qui avait été censuré par le Conseil Constitutionnel, dans une rédaction compatible avec sa décision du 29 juillet 2004, en prévoyant les garanties légales nécessaires.

L'article 11 du projet de loi précise ainsi que, par principe, les données d'infraction ne peuvent pas être « partagées » ou « cédées » mais qu'elles peuvent être traitées par un tiers autre que la victime ou le mis en cause pour son compte. Cette rédaction vise à couvrir le cas d'une société mère qui dispose d'un service juridique afin qu'elle puisse traiter des données d'infractions pour le compte de ses filiales victimes d'infractions, de même pour les sociétés d'assurances ou certaines association pouvant se constituer partie civile.

Les traitements ne pourront en outre pas avoir pour autre finalité que celle de préparer, exercer, suivre une action en justice, ou de faire exécuter une décision de justice rendue. La durée ne pourra excéder cette finalité (résolution amiable, extinction des voies de recours). La communication à un tiers, comme à un avocat, devra obéir aux mêmes conditions.

3.3. Réutilisation des données publiques de nature pénale contenues dans les décisions de justice

3.3.1. Option 1 (écartée) : Maintien du droit existant

Actuellement l'article 9 de la loi n° 78-17 ne permet pas à des entreprises du secteur de la technologie juridique (*Legal technology*) proposant des logiciels de services juridiques de traiter des données pénales à des fins commerciales par exemple.

Il apparaît par conséquence de prévoir une base légale pour prévoir une telle réutilisation au regard des besoins croissants de ce secteur d'activité[92].

3.3.2. Option 2 (retenue) : Permettre une réutilisation des données de nature pénale dans le respect du droit à la protection des données

Pour les motifs énoncés ci-dessus, il est fait le choix de clarifier dans une disposition législative le cadre de la réutilisation des données contenues dans les décisions de justice.

Il s'agit d'apporter de la sécurité juridique aux réutilisateurs, tout en rappelant les obligations qui leur incombent en tant que responsables de traitement par l'insertion de cette disposition dans le texte fondateur en matière de protection de données à caractère personnel.

Il est en outre rappelé la mention de l'interdiction de traitement visant à la ré-identification des personnes concernées comme limite à la réutilisation, ainsi que le prévoit déjà la loi pour une République numérique du 27 octobre 2016.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

Le présent article du projet de loi prévoit, à l'article 9 de la loi n° 78-17, trois nouvelles dérogations à l'interdiction de traitement des données de nature pénale par des personnes autres que l'autorité publique :

- personnes collaborant au service public de la justice (article 9-1°) ;,
- personnes physiques ou morales, en tant que victimes ou mises en cause, aux fins de leur permettre de préparer et le cas échant, d'exercer et de suivre une action en justice (article 9-2°) ;
- réutilisateurs des informations publiques figurant dans des décisions de justice (article 9-5°).

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

L'impact sur les services judiciaires devrait *a priori* est neutre puisque les traitements pour la gestion du contentieux étaient déjà mis en œuvre en pratique grâce à la réserve d'interprétation du Conseil constitutionnel dans sa décision du 29 juillet 2004.

[92] D'après TechCrunch, depuis décembre 2014, « la Legaltech est en plein essor, avec des sociétés qui tentent d'innover sur le marché du droit à tous les niveaux et de toute part ». Rubin, Basha (6 December 2014). "Legal Tech Startups Have A Short History And A Bright Future". TechCrunch. Retrieved 1 May 2015.

4.3. IMPACTS SUR LES PARTICULIERS

L'ouverture des décisions de justice prévue par la loi pour une République numérique trouvera à s'appliquer aux données d'infractions. Cette disposition législative permettra aux acteurs de la *Legaltech* de réutiliser ces données. Les décisions de justice n'étant pas encore toutes diffusées en open data, il n'est pas possible d'évaluer les impacts précis de la réutilisation des données d'infraction.

En tout état de cause, la connaissance du droit par les citoyens justiciables ne pourra en être qu'améliorée, les réutilisateurs évolueront dans un cadre juridique sécurisé et surtout, la protection des personnes dont les données à caractère personnel apparaissent dans des décisions de justice sera davantage garantie.

4.4. IMPACT SUR LES ENTREPRISES

La possibilité pour des personnes morales de droit privé de mettre en œuvre des traitements de données d'infraction afin de leur permettre de préparer et le cas échant, d'exercer et de suivre une action en justice en tant que victime est de nature en renforcer le suivi de leurs dossiers contentieux et précontentieux. La fonction juridique de leur organisation en sera renforcée.

En outre, l'ouverture des décisions de justice prévue par la loi pour une République numérique du 6 octobre 2016 trouvera à s'appliquer aux données d'infractions. Cette disposition législative permettra aux acteurs du secteur de la technologie juridique de réutiliser ces données. Les décisions de justice n'étant pas encore toutes diffusées en *open data*, il n'est pas possible d'évaluer les impacts précis de la réutilisation des données d'infraction.

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 11	Décret en Conseil d'Etat après avis de la CNIL	Définition des catégories de personnes morales de droit privé collaborant au service public de la justice pouvant traiter des données mentionnées à l'article 9 de la loi n° 78-17

ARTICLE 12

TRAITEMENTS ARCHIVISTIQUES

1. CADRE GENERAL

1.1. ETAT DES LIEUX ET DIAGNOSTIC

L'actuel article 36 de la loi n° 78-17 du 6 janvier 1978 modifiée permet la conservation des données à caractère personnel au-delà de la « durée de conservation » dans le traitement initial, lorsque celle-ci s'inscrit dans des finalités historiques, statistiques ou scientifiques.

Lorsque ces données ont la qualité d'archives publiques au regard de l'article L. 211-4 du code du patrimoine, l'article 36 de la loi du 6 janvier 1978 renvoie à l'article L. 212-3 du même code. Cet article précise les conditions de la sélection des données devant être conservées à titre définitif ou pouvant être éliminées. La sélection se fait d'un commun accord entre l'organisme détenteur des données et l'administration des archives du ministère de la culture. A l'issue de cette sélection, les données destinées à être conservées à titre définitif sont transférées dans les services publics d'archives compétents.

Ces données y sont conservées et traitées (classement, inventaire). Elles sont communiquées dans les conditions prévues aux articles L. 213-1 à L. 213-3 du code du patrimoine aux personnes qui en font la demande dans le cadre de recherches historiques, statistiques, scientifiques ou administratives. Les modalités d'accès sont alignées sur celles qui s'appliquent aux documents administratifs en vertu des dispositions du code des relations entre le public et l'administration. Les documents couverts par des secrets ou mettant en cause des intérêts protégés par la loi ne sont communicables qu'à l'expiration de délais prévus à l'article L. 213-2 du code du patrimoine, par exemple 75 ans à compter de la date des documents pour les minutes des notaires ; 25 ans après le décès ou 120 ans après la naissance pour les documents couverts par le secret médical, etc.

Ces traitements sont dispensés de formalités préalables dès lors que leur finalité se limite à assurer la gestion des archives dans le cadre du livre II du code du patrimoine, relatif aux archives.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision du 9 juillet 2008[93], le Conseil constitutionnel a jugé, à propos de l'article 58 de l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel, que :« *Les articles L. 211-3, L. 212-1, L. 212-2, L. 212-3, L. 212-4, L. 213-3, L. 214-1, L. 214-3, L. 214-4, L. 214-5, L. 214-9 et L. 214-10 du code du patrimoine s'appliquent aux archives qui procèdent de l'activité du Conseil constitutionnel. Ces archives peuvent être librement consultées à l'expiration du délai fixé au 1° du I de l'article L. 213-2 du même code* ».

[93] Décision n°2008-566 DC du 9 juillet 2008

Récemment, le Conseil constitutionnel a consacré le droit d'accès aux documents d'archives publiques découlant de l'article 15 de la Déclaration des droits de l'homme et du citoyen de 1789. Il a précisé qu' *: «Il est loisible au législateur d'apporter à ce droit des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi.* (…) » [94].

1.3. CADRE CONVENTIONNEL

Le règlement (UE) 2016/679 autorise la conservation des données au-delà de la durée du traitement initial lorsqu'elles sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sous réserve de la mise en œuvre de conditions et garanties appropriées (article 5.1.e).

Les traitements à des fins de recherche scientifique ou historique, ou à des fins statistiques, sont mis en œuvre par les chercheurs, les universités et les organismes de recherche.

Ils peuvent également être mis en œuvre par des organismes de droit privé qui produisent ou collectent de la documentation et des archives privées afin d'en assurer la transmission aux générations futures et d'en permettre l'exploitation dans le cadre de recherches historiques, scientifiques ou statistiques. Entrent dans cette dernière catégorie des organismes tels que le Mémorial de la Shoah, la Fondation Jean Jaurès, les services d'archives des Églises, de partis politiques ou d'associations et fondations telles ATD-Quart Monde, la fondation Abbé Pierre ou l'association Génériques, association qui se consacre à l'étude de l'histoire de l'immigration.

Les traitements à des fins archivistiques ne peuvent être mis en œuvre que par des services qui ont « *l'obligation légale de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur, de diffuser des archives qui sont à conserver à titre définitif dans l'intérêt public général et d'y donner accès* » (considérant 158 du règlement). En France, ils sont mis en œuvre par les services publics d'archives (Archives nationales, régionales, départementales, communales, service d'archives du ministère des affaires étrangères et du ministère des armées, etc.), qui conservent des archives publiques ou des archives d'origine privée entrées par achat, dépôt, don, legs ou dation.

Les services publics d'archives ont été juridiquement définis par le décret n° 2017-719 du 2 mai 2017 relatif aux services publics d'archives, aux conditions de mutualisation des archives numériques et aux conventions de dépôt d'archives communales[95].

L'article L. 211-2 du code du patrimoine précise que « *la conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de*

[94] Décision n° 2017-655 QPC du 15 septembre 2017.

[95] Article 2 : « Un service public d'archives a pour missions de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur et de diffuser des archives publiques conformément au I du l'article L. 212-4 et aux articles L. 212-6, L. 212-6-1, L. 212-8, L. 212-11, L. 212-12, R. 212-5, R. 212-6 et R. 212-8 [du code du patrimoine] »

la recherche ». Les documents et données archivés constituent donc des sources pour la recherche en histoire, en sciences humaines et dans les autres secteurs de la recherche, mais peuvent aussi être nécessaires dans le cadre de recherches administratives. En effet, des documents, même anciens, peuvent avoir sur le temps long ou retrouver à la faveur d'événements ou de décisions une valeur administrative et probatoire. C'est ainsi par exemple que les archives de la Seconde Guerre mondiale, qui n'étaient depuis plusieurs décennies plus exploitées que par les historiens, ont été nécessaires pour indemniser, dans les années 1990 et 2000, les personnes spoliées pendant le conflit.

Les données traitées à ces fins dérogent au droit à l'effacement prévu à l'article 17 du règlement, dérogation d'application directe.

Conformément à l'article 89 du règlement, les Etats membres peuvent également prévoir, pour les traitements à des fins de recherche scientifique ou historique, ou à des fins statistiques, des dérogations au droit d'accès de la personne concernée (article 15 du même règlement), au droit de rectification (article 16), au droit à la limitation du traitement (article 18), au droit d'opposition (article 21). Les traitements archivistiques pour l'intérêt public bénéficient des mêmes dérogations, auxquelles s'ajoutent les dérogations à l'obligation de notification de l'effacement de données (article 19) et au droit à la portabilité (article 20).

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Les dérogations qui figurent à l'article 89 du règlement permettent aux services publics d'archives de continuer à assurer leurs missions, de conserver et de mettre à disposition des chercheurs, et notamment des historiens et des archives intègres.

La dérogation au droit de rectification (article 16) préserve le caractère intègre et authentique des données. Elle implique également les dérogations au droit d'opposition (article 21) et au droit à la limitation du traitement (article 18) qui pourraient sinon empêcher le traitement de fonds d'archives, dossiers ou documents (collecte, inventaire), et en interdire l'utilisation.

Ces dérogations sont nécessaires à l'exercice de leurs missions par les services publics d'archives dont les spécificités sont rappelées par la déclaration de l'UNESCO de 2011 : « *Les archives consignent les décisions, les actions et les mémoires. Les archives constituent un patrimoine unique et irremplaçable transmis de génération en génération. Les documents sont gérés dès leur création pour en préserver la valeur et le sens. Sources d'informations fiables pour une gouvernance responsable et transparente, les archives jouent un rôle essentiel dans le développement des sociétés en contribuant à la constitution et à la sauvegarde de la mémoire individuelle et collective. L'accès le plus large aux archives doit être maintenu et encouragé pour l'accroissement des connaissances, le maintien et l'avancement de la démocratie et des droits de la personne, la qualité de vie des citoyens (…) C'est pourquoi nous nous engageons à travailler de concert, pour que : (…) les archives soient gérées et conservées dans des conditions qui en assurent l'authenticité, l'intégrité et la plus grande marge d'utilisation (…).* »

Elles sont également nécessaires aux chercheurs à qui elles garantissent l'accès à une documentation intègre, non modifiée, soumise à l'analyse critique et à l'exploitation que leur imposent leurs méthodes et leur éthique professionnelles.

La dérogation au droit d'accès (article 15) a été inscrite dans le règlement dans la mesure où ce droit implique de pouvoir identifier les personnes mentionnées dans l'ensemble des documents et données, ce qui est impossible pour les milliers de kilomètres de dossiers papier archivés et pour les données versées dans les services d'archives dans des formats et selon des modalités qui ne permettent pas de les interroger dans les mêmes conditions que celles qui prévalent lorsque ces données sont exploitées dans la finalité initiale. En effet, les données sont souvent transférées dans les services d'archives « à plat », hors contexte logiciel d'origine.

Si les personnes concernées ne disposent pas du droit d'accès au sens du règlement, elles bénéficient en revanche du droit d'accès déterminé par le code des relations entre le public et l'administration et le code du patrimoine. L'article L. 311-6 de ce code donne aux personnes un droit d'accès aux documents administratifs qui les concernent, même si ceux-ci sont couverts par un secret ou un intérêt protégé par la loi.

Dans les services publics d'archives, ce droit d'accès est permis par l'existence d'instruments de recherche qui décrivent, de manière synthétique, le contenu des fonds d'archives, dossiers et fichiers en s'appuyant sur des normes internationales de description archivistique (ISAD (G), ISAAR (CPF), ICA-ISDF, ICA-ISDIAH).

La dérogation au droit à la portabilité (article 20) est nécessaire dans la mesure où ce droit représenterait une charge excessivement lourde pour les services d'archives, dont les données sont conservées « à plat » dans des formats différents de ceux qui sont utilisés au stade du traitement initial.

La dérogation à l'obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement (article 19) est la conséquence des dérogations au droit à l'effacement, à la rectification et à la limitation du traitement.

2.2. NECESSITE DE LEGIFERER

Il convient d'inscrire en droit national les dérogations d'application non directe relatives aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Ces dérogations, prévues à l'article 89 du règlement, ont été défendues par la France lors de la négociation de ce dernier.

Les traitements à des fins archivistiques dans l'intérêt public, mis en œuvre par les services publics d'archives en application du code du patrimoine, sont aujourd'hui dispensés de formalités préalables en application de l'actuel article 36 de la loi n° 78-17.

Les dérogations nécessaires à la mise en œuvre de ces traitements doivent être inscrites dans la loi pour pouvoir leur apporter des garanties quant aux modalités de leur mise en œuvre.

3. OPTIONS

Les conditions et garanties appropriées relatives aux traitements à des fins archivistiques dans l'intérêt public, mis en œuvre par les services publics d'archives, sont constituées par l'ensemble des dispositions législatives et réglementaires applicables aux archives publiques et aux archives d'origine privée conservées par les services publics d'archives (plus de 300 dispositions) : règles de sélection, de collecte, de mutualisation ; conditions et modalités d'accès (notamment délais de communicabilité) ; conditions de diffusion sur Internet et de réutilisation des données.

Ces conditions sont fixées par le livre II du code du patrimoine, par le code des relations entre le public et l'administration, ainsi que par plusieurs dizaines de dispositions législatives et réglementaires sectorielles relatives à la communication et à la réutilisation des données (code électoral, code de la santé publique, livre des procédures fiscales, code de l'environnement, etc.).

Ces conditions sont également apportées par le respect d'un large corpus de normes, notamment :

- Normes de description signalées au point 2.1
- NF Z42-013 – Archivage électronique.
- NF Z44-022 relative à la modélisation des données pour l'archivage.
- PR NF EN 16893 - Conservation du patrimoine culturel - Nouveaux sites et bâtiments destinés au stockage et à l'utilisation de collections
- NF ISO 11799 Mai 2016 - Information et documentation - Exigences pour le stockage des documents d'archives et de bibliothèques - Information et documentation - Prescriptions pour le stockage des documents d'archives et de bibliothèques
- ISO/TR 19814:2017 - Information et documentation — Gestion des fonds et collections pour les archives et les bibliothèques

Ces conditions sont suffisantes pour ne pas devoir être précisées par décret, s'agissant de traitements mis en œuvre les seuls services publics d'archives dans le cadre de leur mission de service public.

Les traitements à des fins de recherche scientifique ou historique, ou à des fins statistiques, sont en revanche hétérogènes, mis en œuvre par des responsables de traitement aux profils variés et peuvent avoir des finalités différentes (intérêt public, intérêt privé). Ces traitements doivent pouvoir bénéficier de dérogations partielles ou totales aux articles 15, 16, 18 et 21, dont les conditions et garanties appropriées devront être définies précisément. Un décret en Conseil d'État, pris après avis de la CNIL, pourra préciser les dérogations nécessaires, ainsi que les conditions et garanties appropriées.

Ce décret précisera les mesures techniques et organisationnelles qui permettront d'assurer le respect du principe de minimisation des données.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

La disposition projetée permet de maintenir l'état actuel du droit en matière de gestion et d'exploitation des archives. Il modifie l'article 36 de la loi n° 78-17 pour faire référence aux conditions d'application de la limitation des droits prévues par le règlement (UE) 2016/679.

4.2. IMPACT SUR LES FINANCES PUBLIQUES

La disposition projetée garantit le maintien des conditions actuelles de collecte, de conservation, de traitement et de communication des archives, et, de ce fait, n'induit pas de charges supplémentaires.

4.3. IMPACTS SUR LES PARTICULIERS

La disposition projetée garantit aux particuliers et aux générations futures l'accès à des archives intègres.

4.4. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les dispositions projetées garantissent le maintien des conditions actuelles d'exercice de la fonction archives par les collectivités territoriales. Elles ne généreront de ce fait pas de charge supplémentaire pour les services d'archives dont se sont dotées les collectivités (101 services d'archives départementales, 13 services d'archives régionales et plus de 700 services d'archives communales et intercommunales).

4.5. IMPACT SUR LES ENTREPRISES

S'agissant d'archives publiques « définitives » dont la gestion ne peut pas être confiée à un opérateur privé, il n'y a pas d'impact sur les entreprises.

5. CONSULTATIONS ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Le Conseil national d'évaluation des normes a été consulté et a rendu un avis favorable lors de sa séance du 30 novembre 2017.

ARTICLE 13

TRAITEMENTS DE DONNEES DE SANTE

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

L'accès aux données de santé est régi par l'ensemble législatif suivant.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés encadre les traitements de données à caractère personnel, impose des conditions générales de loyauté et de nécessité de la collecte des données, de leur utilisation pour des finalités déterminées, d'exactitude et de limitation dans le temps de leur conservation et reconnaît aux personnes dont les données font l'objet d'un traitement un droit d'information préalable, un droit d'opposition un droit d'accès et un droit de rectification. Cette loi pose, par ailleurs, en son article 8, le principe d'une interdiction de traitement des données personnelles de santé (et d'autres données dites « sensibles »), sauf si les intéressés y ont consenti ou s'il s'agit de dossiers médicaux ou de traitements d'intérêt public dont la nécessité ou les conditions sont prévues par la loi. Sauf dispositions spéciales, ces derniers sont soumis à une autorisation de la Commission nationale de l'informatique et des libertés en vertu de l'article 25. Le chapitre IX de cette loi fixe un régime spécial d'autorisation pour les traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé ; les projets de recherche sont examinés en amont de la CNIL par l'Institut national des données de santé et un comité consultatif composé de chercheurs (le comité d'expertise pour les recherches, les études, et les évaluations dans le domaine de la santé).

La loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal complète ces dispositions en matière de réutilisation des données personnelles détenues par l'administration. Cette réutilisation est permise dans les conditions de l'article 13 de ce texte : ou bien parce que les personnes intéressées y ont consenti, ou bien parce que ces données ont été rendues anonymes, ou bien si une disposition légale ou réglementaire le permet.

La loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé instaure :

- le système national des données de santé (SNDS) qui met à disposition :

« 1° Les données issues des systèmes d'information mentionnés à l'article L. 6113-7 du présent code ;
« 2° Les données du système national d'information inter régimes de l'assurance maladie mentionné à l'article L. 161-28-1 du code de la sécurité sociale ;
« 3° Les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales ;
« 4° Les données médico-sociales du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles ;

« 5° Un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants.
Le SNDS est basé sur les principes suivants : confidentialité et intégrité des données, traçabilité des accès et des autres traitements.

- l'Institut national des données de santé (INDS) qui est chargé de :
« 1° De veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition, garantissant leur sécurité et facilitant leur utilisation dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
« 2° D'assurer le secrétariat unique mentionné à l'article 54 de la même loi ;
« 3° D'émettre un avis sur le caractère d'intérêt public que présente une recherche, une étude ou une évaluation, dans les conditions prévues au même article 54 ;
« 4° De faciliter la mise à disposition d'échantillons ou de jeux de données agrégées mentionnées au V dudit article 54, dans des conditions préalablement homologuées par la Commission nationale de l'informatique et des libertés ;
« 5° De contribuer à l'expression des besoins en matière de données anonymes et de résultats statistiques, en vue de leur mise à la disposition du public.
« Il publie chaque année un rapport transmis au Parlement. ».

Le comité d'expertise pour les recherches, les études et les évaluations (CEREES) dans le domaine de la santé pour les demandes d'autorisation relatives à des études, évaluations, recherches n'impliquant pas la personne humaine.

- les articles L.1461-1 à L1461-7 du code de la santé publique régissent le SNDS.

- l'article L.1462-1 du code de la santé publique régit l'INDS.

- les articles L.1121-1 et suivants du CSP issus de la loi n° 2012-300 du 5 mars 2012 régissent les recherches impliquant la personne humaine en vue du développement des connaissances biologiques ou médicales. La procédure d'accès aux données suppose, dans ce cas, l'avis d'un comité de protection des personnes (CPP), en amont de la décision de la CNIL.

La loi n°2016-1321 du 7 octobre 2016 pour une République numérique est venue modifier les conditions d'autorisation des traitements de données de santé (articles 25 et 27 de la loi informatique et libertés).

De plus, des textes particuliers interviennent :

- les articles L. 161-29 et L. 161-33 du code de la sécurité sociale prévoient la transmission à l'assurance maladie, par les professionnels et établissements de santé, d'informations médicales telles que les codes des actes et des prestations via les feuilles de soins ou les bordereaux de facturation ;

- une réglementation européenne organise les conditions d'accès et d'utilisation des données personnelles, dans le respect de la vie privée. En effet, outre la directive 95/46/CE du 24 octobre 1995 transposée dans la loi n° 78-17 par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, des dispositions similaires quant à la protection des données personnelles sont consacrées à la fois par l'article 8 de la Charte des droits fondamentaux de l'Union européenne en vigueur dans les États membres et par la convention n° 108 du Conseil de l'Europe.

Le règlement (UE) 2016/579 du Parlement Européen et du conseil du 17 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données entre en vigueur le 25 mai 2018, abrogeant ainsi la directive 95/46/CE.

L'article L. 1110-4 régit l'échange et le partage des données entre professionnels :

- l'échange est autorisé entre professionnels mais limité au strict nécessaire à l'action de soin considérée (coordination, continuité des soins, prévention, suivi) ;
- le partage entre professionnels appartenant à la même équipe de soin est autorisé ;
- le partage entre professionnels n'appartenant pas à la même équipe de soin nécessite le consentement préalable de la personne concernée ;
- concernant le partage et l'échange des données la concernant, la personne doit être dûment informée et peut exercer un droit d'opposition.
-

L'article L. 1111-8 régit les hébergeurs de données de santé à caractère personnel : une obligation d'agrément des prestataires d'hébergement s'applique et une obligation de certification est à venir.

L'article L. 1111-8 interdit la cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord des personnes concernées.

L'article L.1111-8-1 stipule : un identifiant national unique (numéro d'inscription au répertoire national d'identification des personnes physiques, RNIPP) est utilisé comme identifiant de santé.

Les articles L. 1111-14 et suivants du code de la santé publique concernent le dossier médical partagé :

- créé sous réserve du consentement exprès de la personne concernée ;
- hébergé conformément à la réglementation sur l'hébergement ;
- alimenté par les professionnels de santé ;
- la personne concernée peut rendre inaccessibles certaines informations ;
- ensemble du dossier accessible au médecin traitant de la personne concernée ;
- dossier accessible aux autres professionnels de santé avec le consentement de la personne concernée ;
- la personne concernée a accès à la totalité de son dossier ainsi qu'aux traces d'accès ;
- l'accès au dossier médical est interdit lors de la conclusion d'un contrat relatif à une protection en matière de santé et ne peut être exigé lors de la conclusion d'un contrat ou de son application.

L'article L. 1111-23 concerne le dossier pharmaceutique :

- créé sous réserve du consentement exprès de la personne concernée ;
- hébergé conformément à la réglementation sur l'hébergement ;
- sauf opposition de la personne concernée, tout pharmacien peut alimenter, consulter le dossier ;
- sauf opposition de la personne concernée, dûment informée, le médecin qui la prend en charge peut consulter le dossier pharmaceutique ;

- la personne concernée a droit à l'obtention d'une copie du contenu de son dossier ainsi qu'aux traces d'accès ;
- la personne concernée a droit à la rectification et à la clôture de son dossier.

1.2. DIAGNOSTIC

L'accès aux données de santé est actuellement régi par de nombreuses dispositions entrainant des difficultés d'interprétation entre l'Etat et la CNIL, et entravant de fait l'accès aux données.

D'une façon générale, cette situation conduit à :

- délivrer des autorisations d'accès au terme de délais trop longs (prorogation systématique du délai de deux mois par la CNIL jusqu'à des délais pouvant atteindre 18 mois, le silence de la CNIL valant refus) et incompatibles avec, d'une part les exigences du monde économique actuel, et d'autre part la performance publique,
- autoriser la libération de données dans des conditions susceptibles de porter atteinte à la vie privée des citoyens, lesquels s'avèrent le plus souvent insuffisamment informés de l'utilisation de leurs données personnelles.
-

S'agissant de la procédure d'accès aux données de santé pour les études, recherches, évaluations n'impliquant pas la personne humaine, il s'agit de la conforter d'autant qu'elle est en cours de mise en place. À ce jour, les délais légaux imposés à l'INDS et au CEREES sont tenus avec un flux de dossiers relativement limité. Il est à craindre, à l'avenir :

- une difficulté d'absorption du flux de dossiers,
- un engorgement de la CNIL (cette dernière ne s'est pas encore prononcée sur les premiers dossiers de la nouvelle procédure).
-

Les procédures simplifiées actuellement prévues par les textes (méthodologies de références, décisions uniques et facilitations d'accès aux jeux de données agrégées et aux échantillons) sont en cours de construction et mériteraient d'être développées pour permettre une fluidification de l'accès aux des données.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

La présente disposition ambitionne de libérer le potentiel d'exploitation des données de santé tout en respectant la vie privée des citoyens.

Il s'agit en particulier de sécuriser les modalités d'accès aux données :

- en simplifiant les procédures d'accès aux données de santé, par le recours plus systématique aux procédures simplifiées, notamment aux référentiels et règlements types pour les traitements de données à caractère personnel dans le domaine de la santé et aux méthodologies de référence pour les traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé,

- en unifiant le cadre juridique d'accès à toutes les données de santé,

- en apportant des garanties supplémentaires aux citoyens,

- en réduisant les délais d'obtention des autorisations délivrées par la CNIL, lorsque le recours à des procédures simplifiées ne peut pas être activé.

2.2. NECESSITE DE LEGIFERER

L'application du règlement (UE) 2016/579 conduit le Gouvernement à mettre la législation française en conformité.

3. OPTIONS ET DISPOSITIF RETENUS

3.1. OPTIONS ECARTEES

Ont été écartées les options suivantes :

- une simplification excessive issue de la suppression de tous les régimes d'autorisation préalable actuels en raison des risques d'atteinte à la vie privée qui découlent de la manipulation des données de santé, laquelle doit être encadrée ;

- une reprise inchangée des dispositions actuelles.

3.2. OPTION RETENUE

L'application, le 25 mai 2018, du règlement conduit le Gouvernement à simplifier et clarifier les procédures d'accès aux données de santé en supprimant les articles 25 et 27 de la loi n° 78-17 lesquels prévoyaient des régimes d'autorisation différents selon les types de données mobilisées (autorisation de la CNIL, décret en conseil d'État pris après motivé de la CNIL, arrêté pris après avis motivé de la CNIL). Le règlement consacre le principe de l'analyse d'impact sur la vie privée laquelle s'applique de fait à tous les responsables de traitement qui manipulent des données de santé.

Les présentes modifications proposées dans le projet de loi visent, d'une part à conserver les procédures d'accès en vigueur pour les traitements à fin de recherche observationnelle (notamment ceux mobilisant le SNDS) et les traitements de données impliquant la personne humaine, et d'autre part à introduire un dispositif général permettant de couvrir tous les traitements de données à caractère personnel dans le domaine de la santé impliquant un intérêt public, une saisine éventuelle de l'INDS et une autorisation de la CNIL.

D'une façon générale, le recours aux référentiels et règlements types et aux méthodologies de référence, homologuées par la CNIL, devient le principe et les demandes de traitement s'inscrivant dans une démarche d'obtention de l'autorisation de la CNIL, l'exception.

Par ailleurs, les procédures simplifiées couvrent désormais des jeux de données plus larges (seuls les jeux de données agrégés et les échantillons y étaient éligibles à ce jour), et les autorisations uniques sont maintenues.

Enfin, le Gouvernement propose de modifier la règle régissant le délai de délivrance de l'autorisation de la CNIL en substituant à la règle du « silence vaut refus » la règle du «silence vaut acceptation ».

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

Le développement de l'utilisation des données de santé doit permettre d'améliorer la connaissance du système de santé par les élus et les citoyens de façon à optimiser la prise en charge sanitaire et sociale.

Il doit également permettre la rationalisation des dépenses de santé grâce à l'optimisation des parcours de soins et des processus de prise en charge des patients.

Enfin, au regard des enjeux du *big data* et de l'intelligence artificielle, l'accès facilité aux données de santé constitue un atout pour la France en terme de positionnement international et d'attractivité économique.

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Les dispositions réglementaires d'application de la loi informatique et libertés devront être adaptées en conséquence, notamment le décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 13 (article 54 de la loi n° 78-17)	Décret en Conseil d'Etat après avis de la commission nationale de l'informatique et des libertés	Modalités de saisine de l'Institut national des données de santé
Article 13 (article 55 de la loi n° 78-17)	Arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés	Liste des organismes ou services chargés d'une mission de service public mettant en œuvre des traitements de données de santé à caractère personnel afin de répondre à une situation d'alerte sanitaire
Article 13 (article 63 de la loi n° 78-17)	Décret en Conseil d'Etat après avis de la commission nationale de l'informatique et des libertés	Composition et fonctionnement du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé

ARTICLE 14

DECISION ADMINISTRATIVE AUTOMATISEE

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La loi n° 78-17 du 6 janvier 1978 a instauré un régime de protection des personnes à l'égard des décisions prises sur le fondement d'un traitement automatisé de données à caractère personnel (articles 10 et 39). Ce régime de protection inscrit dans la loi, à la suite du rapport Tricot de 1975 qui insistait sur « *la nécessité de ne compter sur l'analyse d'un système que comme un instrument de travail parmi d'autres et de ne s'en remettre jamais à ses seules conclusions* », assure la garantie d'une informatique humaine.

La loi proscrit ainsi le profilage automatique pour les décisions de justice. Cet usage est encadré pour les autres décisions produisant des effets juridiques. Ainsi, lorsqu'une décision implique une appréciation sur un comportement humain fondée sur un algorithme établissant le profil d'un individu la personne peut obtenir que l'évaluation soit vérifiée ou contredite par une intervention humaine.

La Commission nationale de l'informatique et des libertés, au travers de ses avis et mises en demeure, a établi une doctrine concernant l'article 10 de la loi n° 78-17. Elle ne prohibe pas l'utilisation d'algorithmes dans la prise de décision, notamment par les administrations, dès lors qu'ils ne sont qu'un simple outil d'aide à la décision : « *compte tenu des enjeux éthiques qu'ils soulèvent, le législateur a prévu que l'utilisation des algorithmes ne pouvait exclure toute intervention humaine* ». Le recours à des algorithmes « *ne [doit] constitu[er] qu'un outil d'aide et d'orientation des travaux des agents* » (délibération n° 2017-226 du 20 juillet 2017).

Dans la mesure où l'Académie française définit un algorithme comme étant une "*méthode de calcul qui indique la démarche à suivre pour résoudre une série de problèmes équivalents en appliquant dans un ordre précis une suite finie de règle*s", les algorithmes peuvent être très divers : une feuille de calcul (type calcul des impôts) ou de *scoring* (par exemple en matière de logement social). La complexité est encore plus grande si l'on considère que la notion juridique de « décision automatisée » est aussi très large.

En complément de la loi du 6 janvier 1978, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a prévu des mesures assurant la transparence des décisions individuelles prises sur le fondement d'un traitement algorithmique. L'article L. 312-1-3 du code des relations entre le public et l'administration prévoit une obligation générale de publication en ligne des règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles. L'article L. 311-3-1 du même code a créé, parallèlement, un régime d'information individuelle l'administration doit informer l'usager, par une mention explicite dans la décision, que ladite décision a été prise sur le fondement d'un

traitement algorithmique et qu'il peut en demander les règles, y compris leur application dans son cas particulier ; les règles définissant le traitement algorithmique ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande.

L'article R. 311-3-1-3 de ce code précise les informations qui doivent être communiquées à l'intéressé s'il en fait la demande :

« 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ;
2° Les données traitées et leurs sources ;
3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ;
4° Les opérations effectuées par le traitement ».

Cette logique de transparence permet de comprendre et d'auditer le traitement et, grâce aux informations obtenues au titre des droits de l'intéressé mentionnés plus haut, de rejouer les opérations effectuées par le traitement.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel s'est prononcé sur l'article 10 de la loi n° 78-17, dans une rédaction antérieure à la modification et à la renumérotation effectuées par la loi n° 2004-801 du 6 août 2004, dans sa décision du 13 mars 2003[96] :« *Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : " Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative* ».

Le commentaire de cette décision précise que « *l'intéressé, dûment prévenu de l'accès au fichier, pourra contester la décision de refus qui lui serait opposée devant le juge compétent* » et que le Conseil d'Etat vérifie la conformité d'une telle décision à l'article 10 de la loi n° 78-17.

Le projet de loi conserve de tels droits évoqués pour la personne concernée : celle-ci est informée de l'utilisation d'un algorithme et dispose des droits de recours, administratif (s'agissant de décisions administratives individuelles) et juridictionnel, de droit commun.

1.3. CADRE CONVENTIONNEL

L'article 22 du règlement (UE) 2016/679, reprenant largement la rédaction de la directive 95/46/CE qu'il abroge, dispose que : *« la personne concernée a le droit de ne pas faire l'objet*

[96] Décision n° 2003-467 DC du 13 mars 2003.

d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative » (point 1).

Ce droit subjectif de ne pas faire l'objet d'une décision automatisée a largement été interprété en France comme prohibant toute décision ayant un effet juridique prise automatiquement par un traitement sans intervention humaine.

Toutefois, ce droit accordé à la personne n'est pas absolu. Le point 2 de l'article 22 du règlement prévoit trois dérogations, lorsque la décision :

- est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement (a) ;
- est autorisée par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée (b) ;
- est fondée sur le consentement explicite de la personne concernée (c).

Dans les cas a) et c), des garanties pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée doivent être également apportées: intervention humaine de la part du responsable du traitement, droit d'exprimer son point de vue et de contester la décision (point 3).

A ce titre, il convient de souligner que le considérant 71 du règlement précise que : « *Toutefois, la prise de décision fondée sur un tel traitement [automatisé], y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement ».*

Les décisions ne peuvent être fondées sur les catégories de données prévues à l'article 9 du règlement (point 4), c'est-à-dire les données sensibles (données biométriques, génétiques, de santé, ethniques, politiques, syndicales, vie sexuelle, religieuse, philosophique), sauf si la personne y consent (point a) du paragraphe 2 de l'article 9) ou que le traitement est nécessaire pour des motifs d'intérêt public important (point g) du même paragraphe).

Les « mesures appropriées pour la sauvegarde des droits et libertés » de la personne ne sont pas définies par le règlement. Le considérant 71 apporte quelques précisions ainsi que les lignes directrices dédiées du G29 :

- droit à l'information (logique sous-jacente, conséquences pour la personne) et à l'explication ;
- droit au recours, y compris, le cas échéant, droit à une intervention humaine et à exprimer son point de vue.

Au-delà de ces droits subjectifs, les responsables de traitement sont invités à contrôler régulièrement pour des biais discriminants (dans la mesure, notamment, où le règlement n'interdit pas strictement le traitement de données « sensibles »).

1.4. ELEMENTS DE DROIT COMPARE

1.4.1 Au Royaume Uni, les traitements automatisés sont autorisés dans le cadre de la loi (pour la fraude fiscale par exemple). L'article 13 du projet de loi d'adaptation du droit national au règlement prévoit de manière transversale les garanties offertes en cas de décisions automatisées prises en application du b) du 2 de l'article 22 :

- notification de la personne dans les meilleurs délais ;
- faculté dans les 3 semaines suivantes de demander un réexamen de la situation ou la prise d'une nouvelle décision qui n'est pas fondée sur le seul algorithme ;
- obligation dans les 3 semaines suivantes de répondre à la demande, ce qui peut impliquer la faculté pour la personne de fournir de nouvelles informations.

Cet article est conforme aux dispositions du *Data Protection Act* de 1998 (article 12(2)b) qui prévoyait le réexamen plutôt que des garanties de transparence, voire un « droit à l'explication », comparable notamment à l'article 39 de la loi française du 6 janvier 1978.

1.4.2 En Allemagne, le paragraphe 6a) du *Bundesdatenschutzgesetz* reprend largement le règlement : la section (2) prévoit la possibilité de déroger par une mesure législative. Le (3) permet aux personnes concernées d'avoir connaissance du mécanisme qui fonde la décision, au sens de la logique sous-jacente.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

Alors que certaines décisions sont d'ores et déjà prises avec une aide algorithmique par les administrations (fraude, affectation, calcul des droits), l'objectif poursuivi est de fixer un cadre juridique protecteur des citoyens mais permettant, dans certains cas, de prendre des décisions administratives individuelles automatisées qui ne requerront plus une intervention humaine a priori et de renforcer la sécurité juridique.

Il convient de prévoir la possibilité d'un recours à une décision automatisée pour les décisions administratives individuelles, à condition que :

- la personne soit clairement informée, par une mention explicite, indiquant la finalité du traitement algorithmique et le droit d'obtenir la communication des règles définissant ce traitement et des principales caractéristiques de sa mise en œuvre, ainsi que les modalités d'exercice de ce droit[97] ;

[97] C'est–à-dire une forme de « droit à l'explication » du traitement, sur le fondement de l'article 39 de la loi n° 78-17 et, principalement, sur celui du décret n° 2017-330 du 14 mars 2017 qui prévoit que, lorsque l'usager exerce son droit, l'administration lui communique, sous une forme intelligible :
1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ;
2° Les données traitées et leurs sources ;
3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ;
4° Les opérations effectuées par le traitement.

- pour être à même d'assurer pleinement cette information, le responsable de traitement maitrise le traitement algorithmique ;
- le droit au recours soit garanti, c'est-à-dire une intervention humaine a posteriori ;
- l'utilisation des données sensibles (qui comprennent notamment les données de santé), permise cependant, sous conditions, par le règlement, soit proscrite.

2.2 NECESSITE DE LEGIFERER

L'article 22 du règlement offre une marge de manœuvre en droit national (point 2. b), pour autoriser la prise de décision automatisée, à condition de prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée,. Le considérant 71 du règlement, par sa formulation (« *la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise* ») permet aux Etats membres d'intégrer dans leur législation des règles de ce type dès lors que les garanties appropriées sont prévues.

Or, l'automatisation de décisions administratives constitue un levier essentiel pour une administration modernisée, permettant de conforter la continuité du service public, en sécurisant sa délivrance, et de sécuriser juridiquement les calculs de droits ou de prélèvements. Les algorithmes apportent une aide pour le traitement et l'analyse de l'information de plus en plus numérisée dans la sphère publique.

L'apparition d'automates hier a permis de renforcer l'efficacité de l'administration tout en permettant aux agents de traiter les situations les plus complexes. Aujourd'hui, les algorithmes sont partout dans la vie quotidienne numérique des Français. Ils déterminent ce que l'on voit sur les plates-formes d'achat en ligne, les réseaux sociaux ou les moteurs de recherche comme l'indique Nohza Boujemaa[98]. Ils sont utilisés par exemple pour fixer une tarification volatile ou organiser les recommandations personnalisées. L'administration utilise déjà largement cette technologie dans bien des situations qui ne donnent pas lieu à polémique tel le calcul des impôts

Ainsi, il apparait nécessaire que la France se dote d'un cadre juridique équilibré permettant aux administrations d'innover en automatisant certaines prises de décisions tout en assurant une totale transparence sur les traitements algorithmiques qu'elle utilise et que les usagers en soient correctement informés, ce qui implique que :

- les algorithmes soient ouverts, auditables et transparents ;
- ils soient « explicables », c'est-à-dire composés de règles dissociables et intelligibles.

Le principal enjeu, comme le relevait le rapport du Conseil d'Etat de 2014[99], est la prohibition d'algorithmes « boîtes noires », qui privent de sens la décision. Sur ce point, d'ailleurs, dans la sphère publique, le secret industriel et commercial ne saurait être opposé, comme c'est le cas dans la sphère privée, ainsi que le soulève l'étude annuelle 2017 du Conseil d'Etat[100]. C'est notamment à cette fin que la plate-forme TransAlgo chargée d'évaluer la responsabilité et la

[98] Article publié dans Le Monde, 2 mai 2017, « La transparence des algorithmes relève des droits civiques » (http://www.lemonde.fr/campus/article/2017/05/02/o21-la-transparence-des-algorithmes-releve-des-droits-civiques_5121201_4401467.html#5ayGvqYycS1oLG0s.99).
[99] Étude annuelle 2014 - *Le numérique et les droits fondamentaux*, p. 233 et s.
[100] Etude annuelle 2017 - *Puissance publique et plateformes numériques : accompagner l'«ubérisation ».*

transparence des systèmes algorithmiques mise en œuvre par l'INRIA en collaboration avec le CNRS, a été créée. C'est également, dans cette logique, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique avait prévu que, dans le cas de décisions administratives individuelles prises sur le fondement d'un traitement algorithmique, l'administration devait être à même de rendre compte précisément des règles utilisées.

3. OPTIONS

3.1. Option 1 (écartée) : Maintien de l'article 10 dans sa rédaction actuelle

La rédaction en vigueur de l'article 10 de la loi n°78-17 ne permet pas de prendre des décisions administratives individuelles sur le seul fondement d'un traitement automatisé de données, une intervention humaine étant requise, entre l'évaluation algorithmique et l'édiction de la décision.

Les algorithmes sont très utilisés dans l'aide à la décision administrative. Une intervention humaine ne semble pas toujours nécessaire pour assurer les droits des personnes concernées et des usagers des services publics, comme par exemple pour le calcul de l'impôt sur le revenu.

Le maintien de cette interdiction absolue ne permet pas de répondre aux évolutions de l'activité administrative qui a de plus en plus recours à des traitements algorithmiques, notamment pour les décisions de masse que la règlementation encadre précisément et dont l'édiction rapide permet la bonne délivrance du service public.

Par ailleurs, l'article doit être adapté au règlement :

- le troisième alinéa de l'article en est la recopie non nécessaire ;
- la notion de profilage est adaptée à la définition du règlement.

Pour l'ensemble de ces raisons, l'écriture actuelle de l'article 10 de la loi n°78-17 n'apparaît plus adaptée.

3.2. Option 2 retenue : Modification de l'article 10 de la loi n° 78-17 pour prévoir dans certaines conditions la prise de décisions administratives individuelles automatisées

Il est proposé d'utiliser la marge de manœuvre prévue au b) du 2 de l'article 22 du règlement (UE) 2016/679 pour ouvrir plus largement la possibilité pour l'administration de recourir à des décisions automatisées (prises sur le fondement d'un algorithme), dans le seul champ des décisions administratives individuelles (et non pour toute décision ayant un effet significatif sur la personne) et à la condition d'offrir d'importantes garanties en contrepartie, en matière d'information pleine et entière des personnes, de maîtrise des traitements de droit au recours et de données traitées (exception des données dites « sensibles » de ce cadre).

L'obligation d'information, issue de l'article L. 311-3-1 du code des relations du public et de l'administration, ne constitue pas simplement une règle de transparence, mais aussi, d'une part, une information proactive de l'usager et, de l'autre, par voie de conséquence directe, une maîtrise sur les règles qui doivent pouvoir être communiquées loyalement à la personne concernée, y compris en cas d'actualisations. Elle est complétée par l'article 39 de la loi de 78 et le règlement qui prévoient également une information de la personne concernée.

Le droit au recours hiérarchique ou gracieux de droit commun implique une garantie d'intervention humaine *a posteriori*[101].
L'enjeu principal, en définitive, n'est pas celui d'une intervention humaine entre la décision algorithmique et sa notification, dont on peut interroger la réelle effectivité, mais :

- d'une intervention humaine *ab initio*, dans l'édiction des règles et dans leur implémentation par l'algorithme : c'est le sens de l'obligation de maîtrise de l'algorithme insérée dans l'article du projet de loi (et qui était déjà affirmée par l'article 16 de la loi pour une République numérique) ;
- et d'une intervention humaine a posteriori pour réformer des décisions dans certaines situations particulières qui seront portées le cas échéant à la connaissance de l'administration.

S'agissant du risque de discrimination ou de biais, l'impossibilité de traiter des données sensibles telles que l'origine ethnique, la religion, l'opinion politique, l'affiliation syndicale ou l'orientation sexuelle apporte une première garantie, que vient compléter l'obligation de maîtrise susmentionnée.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

Le principal impact attendu est la faculté de prendre des décisions administratives automatisées sans intervention humaine par une modification de l'article 10 de la loi n° 78-17, ce qui apportera la sécurisation juridique de certaines décisions pour lesquelles l'intervention humaine est résiduelle.

4.2. IMPACT SUR LES FINANCES PUBLIQUES

Ainsi que le souligne Nozha Boujemaa[102], les services numériques définis et gérés par les algorithmes permettent l'autonomisation du traitement de l'information au-delà de ce que l'humain serait capable de gérer dans un temps comparable, ce qui est une véritable opportunité en termes de gain de performance et d'efficacité de l'exécution de l'action publique.

L'usage des algorithmes est relativement répandu dans le champ des finances publiques, sous deux aspects :

- le calcul des prélèvements comme des droits ;
- la lutte contre la fraude.

La sécurisation des décisions liées au calcul sera améliorée.

[101] On notera que c'est la principale garantie offerte dans l'exemple britannique.
[102] *Acteurs publics*, 8 décembre 2017.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales ne recourent que peu aux algorithmes dans leur prise de décision.

Elles sont toutefois susceptibles de le faire, notamment, en matière de *scoring* pour l'attribution de logements sociaux ou d'affectation (petite enfance).

4.5. IMPACT SUR L'EGALITE ENTRE LES FEMMES ET LES HOMMES ET SUR LES PERSONNES HANDICAPEES

L'automatisation de certaines décisions est susceptible d'avoir un impact positif sur les situations de discriminations, à la condition que les règles des algorithmes prennent en compte *ab initio* le principe de non-discrimination et ses tempéraments particuliers (mise en place de garanties de procédure et de transparence, développement de contrôle des résultats produits par les algorithmes,…).

5. CONSULTATIONS

La Commission nationale de l'informatique et des libertés a été consulté sur cet article.

Le Conseil national d'évaluation des normes a été consulté et a rendu un avis favorable lors de sa séance du 30 novembre 2017.

ARTICLE 15

LIMITATION DES DROITS

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés consacre la section 2 du chapitre V aux droits des personnes à l'égard des traitements de données à caractère personnel.

Elle ne prévoit pas de restriction générale aux droits prévus pour la protection des données à caractère personnel. Des limitations à certains droits sont en revanche prévues à :

- l'article 38 : limitation au droit d'opposition « *lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement* » ;
- l'article 39 en matière de droit d'accès, le responsable de traitement pouvant « *s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.* ». Le droit d'accès ne s'applique pas non plus « *lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique* » ;
- l'article 40 qui prévoit que le droit de rectification et droit à l'effacement ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire pour exercer le droit à la liberté d'expression et d'information, pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit à l'effacement est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement, et enfin à la constatation, à l'exercice ou à la défense de droits en justice.

Ces restrictions sont reprises, précisées ou complétées dans les textes autorisant la création de traitements de données. Par exemple, l'article L. 4123-9-1 du code de la défense prévoit, s'agissant des traitements dont la finalité est fondée sur la qualité de militaires des personnes qui y figurent, que les personnes concernées ne sont averties, en cas de divulgation ou d'accès non autorisé à leurs données, qu'après l'accord du ministère compétent.

1.2. CADRE CONVENTIONNEL

L'article 23 du règlement (UE) 2016/679[103] prévoit une marge de manœuvre importante qui permet aux Etats membres « *par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir* » certaines finalités, missions ou objectifs listés[104].

Les droits visés sont l'ensemble des droits définis à la section 1 du chapitre III du règlement, à savoir, outre les droits déjà prévus par la loi n° 78-17, le droit à l'effacement (article 17 du règlement) et le droit à la portabilité des données (article 20).

Le considérant 73 du règlement précise que : « *Des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données, au droit à la portabilité des données, au droit d'opposition, aux décisions fondées sur le profilage, ainsi qu'à la communication d'une violation de données à caractère personnel à une personne concernée et à certaines obligations connexes des responsables du traitement peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ou de manquements à la déontologie des professions réglementées, et pour garantir d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés pour des motifs d'intérêt public général, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires. Il y a lieu que ces limitations respectent les exigences énoncées par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.* »

---

[103] L'article 13 paragraphe 3, l'article 15 paragraphe 1 et l'article 16 paragraphe 4 de la directive (UE) 680/2016 prévoient des dispositions équivalentes.

[104] *« a) la sécurité nationale;\ b) la défense nationale; \ c) la sécurité publique; \d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; \ e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale; \ f) la protection de l'indépendance de la justice et des procédures judiciaires; \ g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière; h) \ une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g); i) \ la protection de la personne concernée ou des droits et libertés d'autrui; j) \ l'exécution des demandes de droit civil. »*

Par ailleurs, l'article 23 du règlement précité utilise la notion de « mesures législatives ». Le considérant 41 du règlement précise à cet égard que : « *Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée «Cour de justice») et de la Cour européenne des droits de l'homme.* ».

La Cour européenne des droits de l'homme retient également une acception "matérielle" et non "formelle" du terme de « loi ». A ce titre elle y inclut des textes de rang infralégislatif[105].

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

Le projet de loi vise également un objectif de clarification et d'intelligibilité du droit en définissant les conditions dans lesquelles certains traitements ou catégories de traitements sont autorisés à déroger au droit à la communication d'une violation de données.

2.2 NECESSITE DE LEGIFERER

Les droits reconnus en matière de traitements de données à caractère personnel sont définis par la loi 78-17 tout comme les dérogations à ces droits. L'article 23 du règlement permet une marge de manœuvre sur les limitations des droits des personnes concernées..

Le présent projet de loi souhaite compléter les dérogations prévues par la loi n° 78-17, pour les cas dans lesquels la communication d'une divulgation ou d'un accès non autorisé à des données est susceptible de présenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique, et lorsque sont en cause des traitements ou catégories de traitements nécessaires au respect d'une obligation légale ou à l'exercice d'une mission d'intérêt public.

En effet, dans le contexte actuel, les démarches et intentions d'organisations terroristes visant à dérober des données personnelles sensibles constituent une menace grave et crédible. Il est donc souhaitable de prévoir l'absence de communication à la personne concernée de la divulgation de ses données afin que puisse être évalué si la diffusion d'une information sur cette divulgation ou cet accès non autorisé est susceptible de représenter un risque pour la sécurité des personnes, la sécurité publique ou la sûreté de l'Etat. Ce n'est que si ce n'était pas le cas que l'intéressé pourrait être informé de la violation de ces données personnelles.

Des dispositions ont d'ailleurs déjà été adoptées en ce sens dans le code de la défense (cf. articles L. 4123-9-1 et R. 4123-51) pour les traitements dont la finalité exige l'enregistrement de la qualité de militaire.

[105] CEDH, Huvig et Kruslin c/ France, 24 avril 1990, 11801/85 points 27 à 29.

La reconnaissance par le législateur d'un droit à la communication d'une violation de données et l'encadrement du champ et la portée des exceptions à un tel droit participent de la définition des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques au sens de l'article 34 de la Constitution.

3. OPTIONS

3.1. Option 1 (écartée) : Ne rien inscrire dans la loi

Le règlement étant d'application directe, le législateur ne peut se prononcer sur cette mesure et considérer implicitement que c'est directement chaque acte règlementaire qui autorise ou crée un traitement qui peut prévoir les limitations à certains droits.

3.2. Option 2 (retenue) : Prévoir une possibilité de limitation de certains droits dans le respect de l'article 23 du règlement tout en rattachant les dérogations aux traitements ou catégories de traitement

Cette option fixe le principe de l'existence de dérogations au droit à la communication d'une violation de données mentionné à l'article 34 du règlement, en précisant la portée de l'article 23 à un triple titre :

- en proposant de limiter le champ de la dérogation à certaines violations de données (et non à l'ensemble de celles définies à l'article 4.12 du règlement[106]), à savoir la divulgation de données et l'accès non autorisé à celles-ci (uniquement les manœuvres frauduleuses et non les défaillances dont les administrations seraient responsables) ;
- en mentionnant le fait que le besoin de garantir la sécurité nationale, la défense nationale et la sécurité publique ne résulte pas de la nature de certaines données du traitement mais de la communication de la violation des données elle-même. En d'autres termes, ce n'est pas le vol de données qui impose l'absence de notification mais le fait que les personnes « volées » soient averties de ce vol, que le voleur en soit informé et qu'il prenne conscience de la sensibilité des informations détenues ;
- en limitant le champ d'application de cette dérogation aux traitements ou catégories de traitement nécessaires au respect d'une obligation légale ou à l'exercice d'une mission d'intérêt public.

Ce choix reflète celui qui existe actuellement dans la loi n° 78-17 en matière de limitation des droits et celui qui a été retenu pour la transposition de la directive (UE) 280/2016, en son article 70-21 créé par le projet de loi. Il va toutefois au-delà en prévoyant l'édiction d'un décret en Conseil d'Etat pris après avis de la CNIL afin d'encadrer le champ et la portée de ces dérogations.

[106] Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Cette option permet enfin de clarifier la notion de « *mesures législatives* » qui figure dans les deux textes européens, laquelle renvoie, ainsi qu'il a été dit précédemment, à des mesures qui ne sont pas nécessairement adoptées par le Parlement, ainsi que le précisent les considérants 41 du règlement et 33 de la directive.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

Le projet de loi, en complétant l'article 40 de la loi n° 78-17, prévoit la possibilité d'une limitation à être informé des violations d'un traitement de données personnelles, régi par l'article 34 du règlement pour les seuls traitements répondant à une obligation légale, et aux seules fins de protection de la sécurité nationale, de la défense nationale ou de la sécurité publique, .

Il s'agit de permettre aux responsables du traitement de ne pas prévenir la personne dont les données ont fait l'objet d'une violation par un tiers dans des conditions mettant en cause, à raison de données ou à raison de l'emploi de la personne (par exemple s'il s'agit d'un agent des forces de sécurité ou d'un militaire), la sécurité ou la défense, afin de mieux assurer la lutte contre les auteurs de ces violations.

Sont notamment visés par ces dispositions, les traitements comportant des données personnelles à caractère sensible relatives, en particulier, à la qualité de militaire (article 117 de la loi n° 2016-731 du 3 juin 2016) ou à des agents du ministère de la défense occupant des fonctions sensibles (traitements de données de ressources humaines ou du service de santé des armées).

5. CONSULTATIONS ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 15	Décret en conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés	Fixation de la liste des traitements et des catégories de traitements autorisés à déroger au droit à la communication d'une violation de données régi par l'article 34 du, règlement (UE) 2016/679.

CHAPITRE V

VOIES DE RECOURS

ARTICLES 16 ET 17

MODALITES D'EXERCICE DES VOIES DE RECOURS

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

1.1.1 Les voies de recours offertes à la personne concernée

Une personne concernée par un traitement de données dispose de deux voies de recours pour faire valoir ses droits : elle peut déposer un recours auprès de la Commission nationale de l'informatique et des libertés ou auprès de la juridiction compétente (pénale, civile ou administrative).

L'article 11 2° c) de la loi n°78-17 prévoit ainsi que la Commission nationale de l'informatique et des libertés reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements et informe leurs auteurs des suites données à celles-ci. Ce droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés est désormais consacré à l'article 77 du règlement (UE) 2016/679.

Les décisions de la Commission nationale de l'informatique et des libertés au titre de ses missions de contrôle ou de régulation sont susceptibles d'être l'objet d'un recours devant le Conseil d'Etat statuant en premier et dernier ressort (article R.311-1 4° du code de justice administrative). L'article 46 de la loi n°78-17 précise à cet égard que : « *les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.* ».

La loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle a également introduit une nouvelle modalité de recours juridictionnel en créant une action de groupe en matière de protection des données à caractère personnel ouverte devant le juge judiciaire et le juge administratif. Ce recours, sans mandat, permet de solliciter du juge la cessation d'un manquement (article 43 ter de la loi n°78-17). Ce recours ne permet pas, en revanche, d'exercer une action en réparation.

L'article 80.1 du règlement (UE) 2016/679 permet aux personnes concernées de mandater des organisations, des organismes ou des associations pour exercer leurs droits visées aux articles 77, 78 et 79 avec la possibilité de l'étendre au droit d'obtenir réparation si le droit de l'État membre le prévoit.

1.1.2 Les voies de recours offertes à la Commission nationale de l'informatique et des libertés

La Commission nationale de l'informatique et des libertés a également la faculté de saisir la justice, cette faculté est cependant limitée.

Ainsi, le e du 2° de l'article 11 de la loi n°78-17 prévoit qu'elle peut répondre aux demandes d'avis formulées par les juridictions. L'article 1er du projet de loi vise à compléter cet article pour prévoir que la CNIL peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement et de la loi du 6 janvier 1978.

Elle a également la possibilité de dénoncer au procureur de la République les infractions à la loi informatique et libertés, prévues aux articles 226-16 à 226-24 du code pénal (article 11, 2°, e).

Enfin, le président de la Commission nationale de l'informatique et des libertés peut demander, par référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire en cas d'atteinte grave et immédiate aux droits et libertés (article 45-III de la loi n°78-17).

1.1.3 La compétence de la CNIL en cas de transferts de données vers des pays tiers

L'article 70 de la loi n°78-17 octroie à la Commission nationale de l'informatique et des libertés une prérogative en matière de transfert de données vers des Etats non membres de l'Union européenne.

Si la Commission des Communautés européennes a constaté qu'un Etat non membre de l'Union européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration doit délivrer un récépissé avec la mention de l'interdiction de procéder au transfert des données vers cet Etat.

Lorsqu'elle estime qu'un Etat non membre de l'Union européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert de données, la Commission nationale de l'informatique et des libertés doit en informer sans délai la Commission européenne et peut enjoindre au responsable du traitement de suspendre le transfert des données vers cet Etat. Si la Commission européenne constate que l'Etat vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission européenne constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet Etat.

Ces dispositions ont vocation à perdre leur portée dès lors que le régime des déclarations auprès de la Commission nationale de l'informatique et des libertés est supprimé dans le cadre de la mise en conformité de la loi n° 78-17 au règlement (UE) 2016/679.

En revanche, il est proposé, dans le cadre du présent projet de loi, de créer une nouvelle voie de recours pour la Commission nationale de l'informatique et des libertés dans le cadre des transferts de données internationaux, afin de tirer les conséquences de l'arrêt du 6 octobre 2015, par lequel la Cour de justice de l'Union européenne a jugé : « *il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision* »[107].

1.2. CADRE CONSTITUTIONNEL

La nouvelle voie de recours instituée en faveur de la Commission nationale de l'informatique et des libertés tire les conséquences d'un arrêt de la Cour de justice de l'Union européenne.

Il s'agit de permettre à la Commission, lorsqu'elle est saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant dans le cadre d'un transfert de données vers un Etat non membre de l'Union européenne, de demander au Conseil d'État d'ordonner, dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de l'acte approuvé par la Commission européenne ayant permis le transfert, la suspension ou la cessation du transfert de données en cause, le cas échéant sous astreinte, lorsque la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données. Si le Conseil d'Etat partage les doutes de la Commission sur la validité de cet acte, il devra poser une question préjudicielle à la Cour de justice de l'Union européenne en application de l'article 267 du Traité sur le fonctionnement de l'Union européenne.

La disposition ainsi prévue est conforme au cadre constitutionnel national. En effet, le Conseil constitutionnel a rappelé à plusieurs reprises la compétence de la Cour de justice de l'Union européenne pour se prononcer sur la validité et l'interprétation d'un acte adopté par une institution de l'Union européenne[108].

1.3. CADRE CONVENTIONNEL

1.3.1 L'article 58.5 du règlement (UE) 2016/679 dispose que : « *Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement* ».

Le chapitre VIII relatif aux voies de recours, à la responsabilité et aux sanctions prévoit notamment le droit d'introduire une réclamation auprès d'une autorité de contrôle (article 77), le droit à un recours juridictionnel effectif contre une autorité de contrôle (article 78), le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant (article 79),

[107] CJUE, 6 octobre 2015, Maximillian Schrems, C-362/14, considérant 65.
[108] Décision n° 2006-540 DC du 27 juillet 2006, cons. 20 ; Décision 2008-564 DC du 19 juin 2008, cons.45, Décision n° 2010-605 DC du 12 mai 2010, cons.15 et 18.

la représentation des personnes concernées (article 80) et un droit à réparation et responsabilité (article 82).

L'article 55 de la directive prévoit également le droit pour les personnes concernées de mandater un organisme, une organisation ou une association à but non lucratif pour exercer les mêmes réclamation et recours que ceux prévus par le règlement.

1.3.2 La Cour de justice de l'Union européenne a consacré une nouvelle voie de droit par le considérant 65 de la décision Maximillian Schrems du 6 octobre 2015, C-362/14 :

« *63 […] lorsqu'une personne, dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers ayant fait l'objet d'une décision de la Commission au titre de l'article 25, paragraphe 6, de la directive 95/46, saisit une autorité nationale de contrôle d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ces données et conteste, à l'occasion de cette demande, comme dans l'affaire au principal, la compatibilité de cette décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes, il incombe à cette autorité d'examiner ladite demande avec toute la diligence requise.*

64. Dans l'hypothèse où ladite autorité parvient à la conclusion que les éléments avancés au soutien d'une telle demande sont dépourvus de fondement et rejette, de ce fait, cette dernière, la personne ayant introduit ladite demande doit, ainsi qu'il résulte de l'article 28, paragraphe 3, second alinéa, de la directive 95/46, lu à la lumière de l'article 47 de la Charte, avoir accès aux voies de recours juridictionnelles lui permettant de contester une telle décision lui faisant grief devant les juridictions nationales. Eu égard à la jurisprudence citée aux points 61 et 62 du présent arrêt, ces juridictions sont tenues de surseoir à statuer et de saisir la Cour d'une procédure de renvoi préjudiciel en appréciation de validité lorsqu'elles considèrent qu'un ou plusieurs moyens d'invalidité avancés par les parties ou, le cas échéant, soulevés d'office sont fondés (voir, en ce sens, arrêt T & L Sugars et Sidul Açúcares/Commission, C-456/13 P, EU:C:2015:284, point 48 et jurisprudence citée).

65. Dans l'hypothèse contraire, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel, cette même autorité doit, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret, de la directive 95/46, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte, pouvoir ester en justice. À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision. »

Les arrêts rendus par la Cour de justice de l'Union, notamment lorsqu'elle statue à titre préjudiciel comme c'est le cas dans l'arrêt précité, ont une force exécutoire en vertu de l'article 280 du Traité sur le fonctionnement de l'Union européenne.

1.4. ELEMENTS DE DROIT COMPARE

La loi allemande de protection des données[109] a prévu deux dispositions spécifiques, l'une (section 20) concernant le droit au recours juridictionnel prévu à l'article 78 du règlement[110], l'autre (section 21) aménageant la voie de recours définie dans l'arrêté Schrems précité. Dans ce dernier cas, si l'autorité de contrôle estime qu'une décision d'adéquation de la Commission européenne dont dépend la validité d'une décision de l'autorité de contrôle méconnaît la loi, l'autorité de contrôle suspend sa procédure et introduit une demande de décision de justice. Si le juge estime que la décision de la commission est valide, il doit en juger ainsi. Dans les autres cas, il doit pouvoir poser une question préjudicielle en application de l'article 267 du Traité sur le fonctionnement de l'union européenne[111].

L'article 173 de la loi anglaise de protection des données[112] rappelle l'existence de l'action de groupe avec mandat prévu à l'article 80 du règlement. Elle utilise la marge de manœuvre prévue à l'article 80.1 pour permettre une telle action de groupe afin d'exercer un droit à réparation[113].

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

Les dispositions du présent projet de loi doivent permettre au système juridique français de se conformer aux obligations découlant du droit de l'Union européenne, tant le règlement que la jurisprudence de la Cour de justice de l'Union européenne. Cette mise en conformité doit notamment permettre de garantir des voies de droit cohérentes et effectives pour les personnes concernées et renforcer le pouvoir de contrôle de la CNIL.

Ces dispositions, combinées à la possibilité pour la CNIL introduite par l'article 1er du projet de loi de présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement et de la loi du 6 janvier 1978 (cf. supra), visent ainsi à renforcer la

---

[109] Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680

[110] "Recourse to the administrative courts shall be provided for disputes between natural or legal persons and a supervisory authority of the Federation or a Land concerning rights according to Article 78 (1) and (2) of Regulation (EU) 2016/679 and Section 61. (…)".

111 "(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision. (…) 6. In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Administrative Court finds that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice."

[112] Data Protection Bill [HL] 2017-19, Data Protection Bill (HL Bill 66).

113 "173. Representation of data subjects (1) In relation to the processing of personal data to which the GDPR applies— / (a) Article 80 of the GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise certain rights on the data subject's behalf, and / (b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 (right to compensation)."

capacité d'action en justice de la CNIL et garantir le respect effectif des droits des personnes concernées.

2.2 NECESSITE DE LEGIFERER

D'une part, l'article 80 du règlement impose aux Etats membres de prévoir un droit pour les personnes concernées de mandater un organisme, une organisation ou une association afin d'introduire une réclamation auprès d'une autorité de contrôle (article 77), d'exercer un recours juridictionnel contre une autorité de contrôle (article 78) ou contre un responsable du traitement ou un sous-traitant (article 79). Une telle obligation s'impose également en vertu de l'article 55 de la directive.

D'autres modalités de recours relèvent des marges de manœuvre des Etats membres : possibilité d'étendre le mandat défini précédemment afin d'exercer une action en réparation (article 80.1), possibilité pour un organisme, une organisation ou un association, d'exercer les droits définis ci-dessus, indépendamment de tout mandat confié par une personne concernée (article 80.2).

D'autre part, l'arrêt de la Cour de Justice du 6 octobre 2015 précité impose en outre au législateur national de prévoir une voie de droit spécifique permettant à l'autorité de contrôle de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité d'une décision d'adéquation de la Commission européenne, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.

3. OPTIONS

3.1. Introduction d'une action de groupe avec mandat devant l'autorité de contrôle

L'article 80.1 du règlement prévoit une obligation pour les Etats membre d'assurer le droit pour une personne concernée de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit national pour exercer les droits prévus aux articles 77, 78 et 79 du règlement. Une marge de manœuvre est ouverte d'étendre ce droit aux actions en réparation visé à l'article 82 du même règlement.

3.1.1. Option 1 (écartée) : Application directe du règlement sans précision

Afin de permettre aux personnes concernées de connaître l'existence de cette voie de recours, il a semblé important de réaffirmer la possibilité de l'action permise par le règlement, bien que d'application directe. En outre, l'article 80.1 du règlement renvoie au droit de l'Etat membre le soin de déterminer selon quelles modalités une association peut agir avec le mandat.

3.1.2. Option 2 (écartée) : Utiliser la marge de manœuvre de l'article 80.1 du règlement (UE) 2016/679 pour introduire une action avec mandat aux fins de réparation

La loi de modernisation de la justice du XXIème siècle qui a créé une action de groupe en cessation de manquement n'a pas prévu d'étendre le champ de cette action aux fins de réparation.

Les débats parlementaires soulignent l'opposition du législateur national d'étendre l'action de groupe aux demandes en réparation.

Compte-tenu du caractère récent de l'introduction de l'action de groupe dans le droit national, il a donc été décidé de ne pas utiliser la marge de manœuvre prévue à l'article 80.2 du règlement.

3.1.3. Option 3 (retenue) : Ouvrir l'action de groupe obligatoire prévue à l'article 80.1 aux associations déjà prévues au IV de l'article 43 ter

Ainsi qu'il a été dit au point 3.1.1, il revient au droit national de préciser les conditions selon lesquelles un organisme, une organisation ou une association peut, par mandat, exercer les droits prévus aux articles 77, 78 et 79 du règlement. Il en est de même en vertu de l'article 55 de la directive, s'agissant des traitements relevant du champ d'application de cette dernière (nouveau chapitre XIII de la loi n°78-17).

Afin de ne pas complexifier le régime, il est proposé de renvoyer aux organismes et associations déjà mentionnés au IV de l'article 43 ter de la loi n°78-17.

3.2. Introduction d'une représentation sans mandat pour exercer le droit de réclamation et les droits de recours juridictionnel

3.2.1. Option 1 (écartée) : Utiliser la marge de manœuvre prévue à l'article 80.2 du règlement pour l'ensemble des droits

L'article 43 ter de la loi n° 78-17, introduit par la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, en prévoyant une action de groupe, sans mandat, pour faire cesser un manquement par un responsable de traitement subi par plusieurs personnes physiques, organise déjà la marge de manœuvre prévue à l'article 80.2 du règlement s'agissant du droit à un recours effectif contre un responsable de traitement ou un sous-traitant (article 78).

Compte-tenu du caractère récent de ces nouvelles dispositions, il n'a pas été décidé d'étendre la marge de manœuvre prévue à l'article 80.2 du règlement pour l'exercice du droit de réclamation auprès de l'autorité de contrôle (article 77) et du droit de recours juridictionnel contre l'autorité de contrôle (article 78).

Le droit actuel permet déjà, en tout état de cause, à une personne concernée d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (article 11 2°-c) et à toute personne physique ou morale, de contester une décision prise par la Commission au titre de sa mission de contrôle devant le Conseil d'Etat (article R. 311-1 du code de justice administrative).

3.2.2. Option 1 (retenue) : Ne pas modifier le droit existant

Au regard des éléments évoqués précédemment, il a été décidé de ne pas faire usage de la marge de manœuvre prévue à l'article 80.2 du règlement, l'article 43 ter de la loi n° 78-17 permettant déjà de satisfaire une partie des possibilités offertes par le règlement.

Pour résumer, les choix opérés par le présent projet de loi sont les suivants :

Type de recours	Représentation des parties avec mandat (art. 80.1)	Représentation des parties sans mandat (art. 80.2)
Droit de réclamation (art. 77)	Nouvel article art. 43 quater	X
Droit de recours contre l'autorité de contrôle (art. 78)	Nouvel article art. 43 quater	X
Droit de recours contre un responsable de traitement (art. 79)	Nouvel article art. 43 quater	Actuel art. 43 ter
Droit à réparation (art. 82)	X	Sans objet

3.2 : Aménagement d'une voie de recours définie par l'arrêt CJUE - C-362/14

3.2.1. Option 1: Absence de mesure législative

Le droit actuel ne prévoit pas la voie de recours définie dans l'arrêt Maximillian Schrems du 6 octobre 2015 précité, à savoir la possibilité pour la Commission nationale de l'informatique et des libertés de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision d'adéquation de la Commission européenne, à un renvoi préjudiciel aux fins de l'appréciation de la validité de cette décision par la Cour de justice de l'Union européenne.

Une absence de mesure législative exposerait la France à une procédure en manquement, en application des articles 258 à 260 du Traité sur le fonctionnement de l'Union européenne, dès lors qu'il s'agirait d'une méconnaissance d'une obligation découlant d'un texte européen (en l'occurrence, la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), telle qu'interprétée par la Cour de justice.

3.2.2. Option 2 (écartée) : Donner un pouvoir global d'ester en justice à la Commission nationale de l'informatique et des libertés

L'article 58.5 du règlement permet de doter l'autorité de contrôle d'un pouvoir global d'ester en justice. Or la Commission nationale de l'informatique et des libertés, autorité administrative indépendante et non autorité publique indépendante, ne dispose pas de la personnalité morale (article 2 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités

administratives indépendantes et des autorités publiques indépendantes) lui permettant de droit d'agir en justice.

Toutefois, ainsi qu'il a été rappelé dans la première partie, la Commission nationale de l'informatique et des libertés dispose des moyens pour faire appliquer les dispositions du règlement et de la loi n°78-17 : outre les mesures de sanction qu'elle peut prendre pour faire cesser la méconnaissance par les responsables de traitement de leurs obligations, sanctions qui sont sensiblement renforcées par le règlement, elle peut, en cas d'atteinte grave et immédiate aux droits et libertés agir par la voie du référé auprès de la juridiction compétente.

Par ailleurs, outre la situation évoquée dans l'arrêt Schrems précité nécessitant l'instauration d'une voie de recours *ad hoc*, il n'a pas été identifié d'autres situations qui nécessiteraient un pouvoir plus étendu accordé à la Commission nationale de l'informatique et des libertés.

3.2.3. Option 3 (retenue) : Introduction d'une nouvelle voie de recours dans le cadre des transferts internationaux de données

Le nouvel article 45 quinquies de la loi n° 78-17 aménage ainsi une voie de recours pour la Commission nationale de l'informatique et des libertés dans le cadre des transferts de données vers un Etat membre de l'Union européenne, conformément à l'arrêt Schrems précité.

Ainsi, lorsqu'elle sera saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale de l'informatique et des libertés pourra demander au Conseil d'Etat d'ordonner, dans l'attente de l'appréciation par la Cour de justice de l'Union européenne, qu'il aura saisi à titre préjudiciel s'il partage des doutes de la CNIL, de la validité d'une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679, la suspension ou la cessation du transfert de données en cause, le cas échéant sous astreinte. La CNIL devra alors assortir ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de tels actes adoptés par la Commission européenne.

Afin de donner un plein effet utile à cette voie de recours, et dans un souci de cohérence et de protection accrue des données à caractère personnel, il a été fait le choix d'élargir cette voie de recours à l'ensemble des actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 du règlement (UE) 2016/679, et pas uniquement les décisions d'adéquation : clause-type de protection des données, code de conduite, mécanisme de certification. Cette nouvelle voie de droit est également étendue à l'égard des décisions d'adéquation de la Commission européenne prises sur le fondement de l'article 36 de la directive (UE) 2016/680, lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle.

Le choix du Conseil d'Etat pour connaître de cette nouvelle voie de recours, par dérogation à la compétence de premier ressort des tribunaux administratifs, a été fait en considération d'une bonne administration de la justice. Actuellement, le Conseil d'État est compétent pour connaître, en premier et dernier ressort, des décisions prises par la Commission nationale de l'informatique et des libertés au titre de sa mission de contrôle. La décision prise par la Commission, après que

la Cour de justice de l'Union européenne se sera prononcée sur la question préjudicielle dont elle aura été saisie, relèvera de la compétence du Conseil d'Etat en vertu de l'article R. 311-1 du code de justice administrative. En outre, ce nouveau recours, qui porte sur une question sensible relative à la protection des données à caractère personnel transférées vers un pays tiers, suppose qu'il soit statué rapidement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'action de groupe avec mandat devant la Commission nationale de l'informatique et des libertés est de nature à limiter le nombre de réclamations individuelles lorsque la violation d'un responsable de traitement ou d'un sous-traitant concerne de nombreuses personnes concernées.

Le projet de loi crée une nouvelle voie de recours devant le Conseil d'État. Cet aménagement permettra une voie de recours effective et rapide dans l'attente de la décision de la Cour de justice de l'Union européenne se prononçant sur la validité d'un acte de la Commission européenne permettant un transfert de données international.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

L'action de groupe avec mandat devant la Commission nationale de l'informatique et des libertés est de nature à diminuer le nombre de décisions de la Commission nationale de l'informatique et des libertés, puisque plusieurs personnes concernées par un traitement feront l'objet d'une seule décision. Par conséquent, le nombre de recours contentieux devrait être diminué, puisqu'une seule décision de la Commission nationale de l'informatique et des libertés et non plus des dizaines, voire des centaines sur le même traitement fera l'objet d'un seul et même recours devant le juge. L'impact sur les services judiciaires devrait donc être une diminution du nombre de contentieux. A ce stade, en l'absence d'action de groupe en matière de protection des données, il n'est pas possible d'évaluer l'impact de la création de cette action par la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^{ème} siècle.

La création de la voie de recours prévue par l'arrêté Schrems précité qui concerne les transferts de données internationaux devrait concerner un contentieux exceptionnel. En effet, à ce jour, la Cour de justice de l'Union européenne n'a eu à se prononcer sur la validité d'une décision d'adéquation suite à un renvoi par une juridiction nationale dans le cadre d'une demande d'une autorité de contrôle qu'une seule fois, en l'occurrence dans le cadre de l'arrêt Schrems. L'impact sur les services judiciaires devrait donc être minime puisque exceptionnel.

4.3 IMPACTS SUR LES PARTICULIERS

Ces mesures créant de nouvelles voies de recours permettront de faire respecter les droits et obligations issus du règlement (UE) 2016/679 et de la loi n°78-17 relative à l'informatique et aux libertés.

4.4 IMPACT SUR LES ENTREPRISES

Les dispositions, en renforçant les voies de recours offertes aux personnes concernées, augmentent en contrepartie le risque contentieux pour les entreprises responsables de traitement ou leurs sous-traitants.

En revanche, ainsi qu'il a été dit précédemment, le projet de loi n'a pas prévu de faire usage de la marge de manœuvre prévue à l'article 80.1 du règlement en étendant l'action du groupe dans le cadre du droit à un recours juridictionnel contre un responsable de traitement ou un sous-traitant au droit à réparation prévu à l'article 82 du même règlement.

5. CONSULTATIONS

La Commission de l'informatique et des libertés a été consultée sur ces articles.

Le Conseil supérieur des tribunaux administratifs et des cours administratives d'appel a été saisi en application de l'article L. 232-3 du code de justice administrative, dès lors que la nouvelle voie de recours prévue par l'arrêté Schrems, en confiant la compétence au Conseil d'Etat pour connaître de ce recours, déroge à la compétence de premier ressort des tribunaux administratifs. Il a émis un avis favorable lors de sa séance du 7 novembre 2017.

La commission supérieure du Conseil d'Etat a également été saisie sur cette même disposition, en application de l'article L. 312-2 du code de justice, dès lors que la nouvelle voie de recours confie au Conseil d'Etat un nouveau type de contentieux. Elle a émis un avis favorable le 1er décembre 2017.

TITRE III

DISPOSITIONS PORTANT TRANSPOSITION DE LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIVE A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR LES AUTORITES COMPETENTES A DES FINS DE PREVENTION ET DE DETECTION DES INFRACTIONS PENALES, D'ENQUETES ET DE POURSUITES EN LA MATIERE OU D'EXECUTION DE SANCTIONS PENALES, ET A LA LIBRE CIRCULATION DE CES DONNEES

ARTICLES 18 ET 19

PRESENTATION GENERALE ET DEFINITIONS

La transposition de la directive (UE) 2016/680 appelle les observations générales suivantes, qui seront complétées par des analyses spécifiques aux quatre sections du nouveau chapitre XIII introduit dans la loi de 1978, et qui sont relatives aux dispositions générales (section 1), aux obligations incombant aux autorités compétentes et aux responsables de traitements (section 2), aux droits des personnes concernées (section 3) et aux transferts de données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des Etats non membres de l'Union (section 4).

La présente partie de l'étude d'impact comporte ainsi des observations de nature générale sur la directive, tout en traitant plus particulièrement de la question des définitions et de la technique législative retenue pour procéder à la transposition.

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. GENESE DE LA DIRECTIVE

1.1.1. HISTORIQUE DE L'ELABORATION DE LA DIRECTIVE

En 1995, l'Union européenne s'est dotée pour la première fois, avec la directive 95/46, d'un cadre juridique destiné à assurer d'une part, la protection des données personnelles des personnes résidant sur son territoire et, d'autre part, la libre circulation de ces données. Le champ d'application de la directive 95/46 était alors circonscrit au domaine communautaire et ne concernait pas le pilier interétatique relatif à la justice et aux affaires intérieures (JAI). Elle a par la suite été complétée par plusieurs instruments ayant pour objet d'assurer la protection de catégories de données particulières, ou d'assurer la protection des données personnelles dans le cadre de traitements de données spécifiques.

Dans le cadre du pilier JAI, la nécessité de disposer de règles relatives aux traitements à des fins de prévention, de détection, d'enquêtes, de poursuites ou d'exécutions des sanctions en matière pénale (fichiers de souveraineté) s'est imposée à la suite des attentats londoniens en 2005. Les État membres ont donc adopté la décision-cadre 2008/977, dont le champ était toutefois limité aux échanges entre États membres ou État membres et États tiers à l'Union tandis que les traitements de fichiers nationaux restaient soumis aux seules législations des États membres.

Le 25 janvier 2012, après avoir hésité à présenter un texte unique, révisant à la fois la directive 95/46 et la décision-cadre 2008/977, et probablement compte tenu des difficultés juridiques et politiques liées notamment à l'existence des protocoles du Royaume-Uni, de l'Irlande et du Danemark, la Commission a présenté deux projets distincts relatifs à la protection des données : d'une part, une proposition de règlement révisant la directive 95/46 et concernant principalement les fichiers civils et commerciaux et, d'autre part, un projet de directive, révisant la décision-cadre 2008/977 concernant les fichiers de souveraineté et incluant les traitements nationaux de fichiers des États membres.

1.1.2. NEGOCIATIONS

Le Conseil européen d'octobre 2013 a demandé que les travaux sur le paquet protection des données puissent s'achever avant la fin de l'année 2015. Afin de respecter cette échéance, les présidences grecque, italienne, et lettone ont fait de ces textes une priorité, ce qui a permis d'aboutir à l'adoption d'une orientation générale sur l'ensemble du texte de la proposition de règlement au Conseil JAI du 15 juin 2015.

Le trilogue avec le Parlement européen, qui a pour sa part débuté ? son mandat en mars 2014, a démarré dès la fin de la Présidence lettone, le 24 juin 2015, et s'est poursuivie sous la Présidence luxembourgeoise, tout au long du second semestre 2015, avec pour objectif de clore le trilogue avant la fin de l'année 2015.

Les discussions sur la proposition de directive étaient nettement moins avancées puisqu'aucune disposition n'avait encore fait l'objet d'un accord politique, les présidences successives ayant largement privilégié les discussions sur la proposition de règlement. Une seule réunion de travail avait ainsi été organisée sous présidence lettone.

1.1.2.1. POSITION FRANÇAISE LORS DES NEGOCIATIONS

La France souhaitait que les travaux sur la directive aboutissent au même titre que ceux sur le règlement, tout en considérant que la réforme de la directive 95/46 et celle de la décision-cadre 2008/977 devaient rester deux exercices distincts, les enjeux en matière de fichiers de souveraineté étant très différents de ceux en matière de données à usage civil ou commercial. La France s'est montrée à cet égard attentive à la question de la délimitation des champs d'application respectifs du règlement et de la directive, les règles applicables aux traitements de données personnelles étant différentes selon l'instrument dont ils relèvent. Ainsi, certains fichiers de police administrative ayant pour objet la prévention des menaces pour la sécurité publique (par exemple le fichier des interdictions de stades) devaient continuer, à l'issue des trilogues, de relever de la directive plutôt que du règlement. En outre, les activités relevant de la sécurité

nationale et du renseignement devaient rester exclues des champs du règlement et de la directive et demeurer de la compétence exclusive des États membres.

En ce qui concerne la directive relative aux fichiers de souveraineté, la France a toujours milité en faveur d'un haut niveau de protection des données, tout en attachant la plus grande importance à ce que les données relatives à la coopération judiciaire pénale et policière et, plus généralement, celles contenues dans les fichiers dits de souveraineté, fassent l'objet de dispositions particulières, compte tenu d'une part de leur finalité, d'autre part de la nature publique du destinataire final des données transmises.

À cet égard, la France était favorable à la délimitation qui était agréée dans le texte du règlement par renvoi à la directive, et qui était destinée à garantir que la directive s'applique à l'ensemble des activités de police et que les traitements de données dans le domaine de l'asile et de l'immigration, qui relevaient de la directive 95/46, continuent de relever du règlement.

Ainsi, la France a estimé que les dispositions relatives aux droits des personnes concernées, qui étaient calquées sur les dispositions correspondantes de la proposition de règlement, n'étaient pas tout à fait adaptées aux domaines spécifiques des activités policières et judiciaires et ne permettraient donc pas à ces autorités de mener leurs activités efficacement.

Les dispositions qui ont soulevé le plus de difficultés pour la France furent celles relatives aux transferts de données à des pays tiers. En particulier, la France était vigilante à ce que les États membres n'aient pas, comme proposé dans le texte initial, à renégocier tous leurs accords bilatéraux existants, après l'entrée en vigueur de la directive.

1.1.2.2. POSITION DES AUTRES ETATS MEMBRES LORS DES NEGOCIATIONS

De nombreuses délégations ont marqué une opposition ferme à l'inclusion dans son champ d'application des traitements de données purement internes, alors que la décision-cadre 2008/977 ne s'appliquait qu'aux traitements de données transnationaux. Certaines de ces délégations, dont l'Allemagne, ont un temps fait valoir l'absence de base juridique permettant une telle harmonisation.

L'unanimité des délégations s'était également opposée aux dispositions de ce texte relatives aux échanges de données avec des pays tiers, considérées comme trop restrictives car transposant à la matière pénale des règles prévues en matière civile et commerciale.

De même, l'obligation de renégocier tous les accords internationaux et bilatéraux qui n'étaient pas en conformité avec la nouvelle directive était jugée irréaliste et inopportune.

Concernant le champ d'application de cet instrument, lors des dernières discussions techniques sur cette question, un consensus s'est dégagé en faveur d'une rédaction qui permettait d'inclure les traitements de données à des fins de protection des menaces pour la sécurité publique et de prévention de telles menaces dans le champ d'application, ce qui permettait de soumettre les fichiers mixtes des États membres aux mêmes règles de protection des données, tout en maintenant les traitements de données en matière d'asile et d'immigration dans le champ du règlement.

1.2. CONTENU DE LA DIRECTIVE

Ce contenu est plus précisément détaillé dans les analyses consacrées aux 4 sections du nouveau chapitre XIII inséré dans la loi de 1978.

Toutefois, il convient ici d'observer que la directive, afin d'assurer le même niveau de protection pour les personnes physiques à l'aide de droits opposables dans l'ensemble de l'Union et d'éviter que des divergences n'entravent les échanges de données à caractère personnel, précise dans son article 3 la définition de certains termes, à savoir celle :

- des «données à caractère personnel» comme toute information se rapportant à une personne physique identifiée ou identifiable alors dénommée « personne concernée », autrement dit qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

- du «traitement» comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

- de la «limitation du traitement» comme le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur;

- du «profilage» comme toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne;

- de la «pseudonymisation» comme le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, conservées séparément et garantissant que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

- du «fichier» comme tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés;

- d' « autorité compétente», définie comme :

* toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou
* tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

- du «responsable du traitement» comme étant l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;

- du «sous-traitant» comme étant la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

- du «destinataire» comme étant la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers, à l'exception néanmoins des autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit d'un État membre ;

- de la «violation de données à caractère personnel» comme étant une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

- des «données génétiques» comme les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

- des «données biométriques» comme les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

- des «données concernant la santé» comme les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

- de l'«autorité de contrôle» comme étant une autorité publique indépendante qui est instituée par un État membre;

- de l'«organisation internationale» comme étant une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

Des définitions exactement similaires figurent également dans l'article 4 du règlement (UE) 2016/679 (la directive comportant toutefois des définitions qui lui sont propres comme sur les autorités compétentes, et le règlement comportant un nombre plus important de définitions).

1.3. CONFORMITE AU DROIT NATIONAL

Seule est examinée ici la question des définitions.

L'article 2 de la loi informatique et libertés précise les définitions des notions de donnée à caractère personnel, de traitement et de fichier.

Ainsi, constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Il est par ailleurs précisé que pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne, et que la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Les articles 3 I et 35 de loi informatique et libertés précisent également les définitions de responsable du traitement, de sous-traitant et de destinataire.

L'article 3 I définit le responsable d'un traitement de données à caractère personnel comme étant, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

Son II définit le destinataire d'un traitement de données à caractère personnel comme toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du

traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

L'article 35 prévoit que toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant.

L'article 34 bis précise que la violation de données à caractère personnel s'entend, dans le cadre de l'application du présent article, de toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

Enfin, l'article 11 de la loi prévoit, conformément aux exigences européennes d'indépendance de l'autorité de contrôle, que la Commission nationale de l'informatique et des libertés est une autorité administrative indépendante.

Le droit national est donc conforme sur les définitions des données à caractère personnel, du traitement, du fichier, du responsable du traitement, du sous-traitant, du destinataire et de l'autorité de contrôle.

Les quelques variantes, telles que les termes de structuration ou de limitation du traitement, restent en effet de pure forme et sans conséquence sur le fond.

En revanche, la notion française de violation de données à caractère personnel, uniquement applicable aux données personnelles faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques, n'apparaît pas suffisante au regard des exigences européennes.

De même, les notions nouvelles de la directive relatives à la limitation du traitement, au profilage, à la pseudonymisation, aux données génétiques, biométriques et de santé, et à l'organisation internationale devront faire l'objet d'une transposition.

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Afin de mettre notre droit en conformité avec les notions nouvelles définies par l'article 3 de la directive (notions de limitation du traitement, de profilage, de pseudonymisation, de violation de données à caractère personnel, des données génétiques, biométriques et de santé et d'organisation internationale) , le dernier alinéa du nouvel article 70-1 crée par le présent projet de loi prévoit que les définitions identiques de ces notions prévues par l'article 4 du règlement (UE) 2016/679 sont alors applicables. .

La définition d'autorité compétente est, quant à elle, reproduite dans le 2° de l'article 70-1, d'une part parce qu'elle est propre à la directive, d'autre part parce qu'elle participe de la délimitation du champ d'application de cet instrument.

S'agissant des règles de fond, elles sont insérées dans un nouveau chapitre XIII de la loi de 1978, créé par l'article 19 du présent projet de loi.

2.2 NECESSITE DE LEGIFERER

L'objectif du projet de loi tendant à mettre notre droit national en conformité avec les exigences énoncées par la directive, impose à la fois d'adapter les règles de fond concernant les traitements entrant dans son champ d'application.

3. OPTIONS

3.1. MODALITES GENERALES DE TRANSPOSITION DE LA DIRECTIVE DANS L'ARCHITECTURE DE LA LOI INFORMATIQUE ET LIBERTES

3.1.1. Option 1 (écartée sauf exception) : Intégrer les règles relatives aux traitements pénaux au fur et à mesure des articles de la loi de 78

Il aurait pu être envisagé, à l'instar de ce qui est fait pour la mise en conformité de la loi de 1978 avec le règlement UE, de « répartir » le contenu des dispositions spécifiques aux traitement pénaux en les « égrenant » tout au long de la loi de 1978, en complétant tel ou tel article de cette loi par des alinéas supplémentaires (mais sans pouvoir procéder par remplacement des dispositions actuelles, car elles devaient continuer de s'appliquer aux traitements qui sont hors du champ du droit de l'Union) ou en insérant après tel ou tel article un nouvel article dérogatoire par rapport au précédent.

Cela aurait imposé, pour chacun de ces ajouts, de préciser qu'il ne s'applique qu'aux traitements pénaux tels que définis par un nouvel article X reprenant les définitions de la directive (ce que fait l'article 70-1 dans la version actuelle du projet de loi).

Une telle solution aurait été particulièrement complexe et la compréhension du droit applicable n'en aurait nullement été améliorée pour les justiciables.

Par ailleurs, d'un point de vue légistique, la dimension des dispositions du projet de loi aurait plus que doublée, puisque pour chacune des dispositions, il aurait dû être non seulement indiqué qu'elle ne concernait que les traitements pénaux, mais également précisé de quelle façon celle-ci était intégrée au sein de la loi de 1978.

Pour toutes ces raisons, cette solution n'a pas été retenue dans son principe.

Toutefois, s'agissant de certaines dispositions par nature communes au règlement et à la directive, les dispositions transposant des articles de la directive ont été insérées dans des articles généraux de la loi de 1978.

Ainsi, l'article 11 de la loi de 1978 qui traite des missions de la CNIL est modifié par l'article 1er du projet de loi pour prévoir dans le i) du II qu'elle peut établir une liste des traitements susceptible de créer un risque devant faire l'objet d'une consultation préalable conformément à l'article 70-4 (ce qui est une conséquence de l'article 28 de la directive).

De même, l'article 44 de la loi de 1978 qui traite des pouvoirs de la CNIL est modifié par l'article 4 du présent projet pour indiquer que dans l'exercice de son pouvoir de contrôle portant non seulement sur les traitements relevant du règlement (UE) 2016/679 mais également sur ceux relevant de la présente loi, et donc relevant de la directive, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions (conformément à l'article 45 de la directive).

De même encore, le nouvel article 43 quater créé par l'article 16 du projet prévoit que la personne concernée peut mandater une association ou une organisation mentionnée au IV de l'article 43 ter aux fins d'exercer ses droits en son nom pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable du traitement ou le sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du chapitre XIII (conformément à l'article 55 de la directive).

Enfin, l'article 43 quinquies, inséré par l'article 17 et qui tire les conséquences de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015, étend les recours à la contestation des décisions d'adéquation prises sur le fondement de la directive afin de permettre la saisine du Conseil d'Etat d'une question préjudicielle à la Cour de justice de l'Union européenne permettant d'apprécier la validité d'une décision d'adéquation prise sur le fondement de la directive.

3.1.2. Option 2 (retenue). Insérer dans la loi de 1978 un chapitre spécifique aux traitements pénaux

La transposition de la directive dans la loi de 1978 ne pouvait raisonnablement pas se faire d'une autre façon que celle retenue par le projet, qui, tout en modifiant ou complétant certains articles de la loi, consiste pour l'essentiel à regrouper les règles spécifiques aux traitements pénaux relevant de la directive dans un chapitre dédié comportant une vingtaine d'articles.

Cette solution est non seulement plus simple et plus lisible, mais elle anticipe la « recodification » globale de la loi de 1978 à laquelle il sera procédé par ordonnance, et qui est indispensable afin d'assurer la meilleure lisibilité possible du droit des traitements (avec un plan comportant nécessairement, et dans cet ordre, au moins les quatre parties suivantes : Dispositions communes ; dispositions concernant les traitements relevant du règlement ; dispositions concernant les traitements relevant de la directive ; dispositions concernant les traitement ne relevant pas du droit de l'Union – ces intitulés n'étant pas nécessairement ceux qui seront retenus pour ces parties mais indiquant ce que sera leur contenu).

3.2. MODALITES GENERALES DE TRANSPOSITION DE LA DIRECTIVE PAR RAPPORT AU REGLEMENT (UE) 2016/679

3.2.1. Option 1 (écartée) : ne pas opérer de renvoi au règlement UE (écartée)

Bien que le règlement (UE) 2016/679, aux termes de son article 2, ne s'applique pas aux traitements de données à caractère personnel relevant du champ de la directive (UE) 2016/680, certains articles de la directive contiennent des dispositions strictement ou quasiment identiques à celles du règlement.
Si la Cour de justice de l'Union européenne censure le simple renvoi général au droit de l'Union européenne en guise de transposition[114], le Gouvernement estimeque des renvois précis à certaines dispositions du règlement peuvent valablement transposer des dispositions de la directive.

L'option de ne pas opérer de renvoi au règlement UE a donc été écartée.

.

3.2.2. Option 2 (retenue) : opérer certains renvois au règlement UE L'option d'opérer des renvois précis aux dispositions strictement identiques de la directive et du règlement a été retenue.

Cette option permet d'éviter des redondances, qui auraient pu à tort laisser penser que les dispositions dérogatoires du nouveau chapitre XIII de la loi informatique et libertés étaient différentes de celles du règlement.

Ainsi, le nouveau chapitre XIII qui transpose la directive renvoie à certaines dispositions du règlement pour les définitions des termes employés, les règles relatives au sous-traitant, les obligations imposées au responsable du traitement et au sous-traitant d'assurer la sécurité des données personnelles, de coopérer avec la Commission nationale de l'informatique et des libertés et de notifier à la commission et à la personne concernée des violations de données personnelles.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

L'impact juridique de la réforme consiste dans l'insertion dans la loi de 1978 d'un chapitre XIII (qui conduit à décaler l'actuel chapitre XIII), et dans la modification des actuels articles 32, 41 et 42 de la loi.

5. CONSULTATION ET MODALITES D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

[114] CJCE, 20 mars 1997, Commission contre Allemagne, C 96/95, Rec. p. 1653.

La réforme s'appliquera le 25 mai 2018, conformément à l'article 24 du projet de loi.

Ces dispositions seront applicables sur l'ensemble du territoire, hors les collectivités d'outre-mer soumises au principe de spécialité, pour lesquelles l'extension se fera par ordonnance

ARTICLE 19 SECTION 1

DISPOSITIONS GENERALES

1. ETAT DES LIEUX

1.1 Conformité du droit français à la directive sur les droits des personnes concernées par les données personnelles

1.1.1 Texte de la directive

1.1.1.1 Champ d'application de la directive

La directive 2016/680 remplace la décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Contrairement à l'instrument précité, son champ d'application n'est pas limité aux échanges de données à caractère personnel dans le cadre de la coopération en matière pénale, mais s'étend à tous les traitements de telles données y compris ceux ne présentant aucun caractère transfrontalier.

La directive s'applique, aux termes de ses article 1 et 2, aux traitements de données à caractères personnel par les autorités compétentes des Etats membres aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Elle ne s'applique en revanche pas, comme le précise son article 2, aux traitements mis en œuvre dans le cadre d'une activité qui se situe hors du champ du droit de l'Union européenne (activités des services de renseignement notamment). La directive ne s'applique pas non plus au traitement de données effectué par les institutions européennes, qui sont soumises au règlement 45/2001.

L'autorité compétente au sens de l'article 3 de la directive correspond à :

- toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

- ou à tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

L'articulation entre la directive et le règlement (UE) 2016/679 s'opère conformément aux considérants 11 et 12 de la directive.
Aux termes du considérant 11, « *les autorités compétentes peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive ». « Lorsqu'un tel organisme ou une telle entité traite des données à caractère personnel à des fins autres que celles prévues dans la présente directive, le règlement (UE) 2016/679 s'applique. Par conséquent, le règlement (UE) 2016/679 s'applique lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques et conformément au droit des États membres ».*

« Un organisme ou une entité qui traite des données à caractère personnel pour le compte de ces autorités dans le cadre du champ d'application de la présente directive devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables aux sous-traitants en vertu de la présente directive, le règlement (UE) 2016/679 continuant de s'appliquer aux traitements de données à caractère personnel par le sous-traitant en dehors du champ d'application de la présente directive ».

Le considérant 12 indique notamment que relèvent de la directive les traitements concernant des « *activités menées par la police ou d'autres autorités répressives [qui] sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non».* Il précise que *« ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple les activités de police lors de manifestations, de grands événements sportifs et d'émeutes»,* et que *« parmi ces activités figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale ».* Il indique en revanche, qu'entrent dans le champ d'application du règlement, pour autant qu'ils relèvent du droit de l'Union, les traitements par lesquels *« les États membres [confient] aux autorités compétentes d'autres missions qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ».

Le champ d'application de la directive est donc déterminé par deux conditions cumulatives :

- l'une porte sur l'autorité chargée de traiter les données à caractère personnel, qui doit être une autorité compétente au sens de l'article 3 de la directive ;

- l’autre sur les finalités du traitement, qui doit être effectué aux fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

A défaut de l’une des deux conditions et pour autant que le traitement relève du droit de l’Union, le règlement (UE) 2016/679 s’applique.

L’article 2 du règlement confirme que cet instrument ne s'applique pas au traitement de données à caractère personnel effectué « *d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces* », terminologie qui correspond très exactement au champ d’application de la directive.

Le considérant 19 du règlement précise cette exclusion en indiquant que « *La protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil (1). Les États membres peuvent confier à des autorités compétentes au sens de la directive (UE) 2016/680 des missions qui ne sont pas nécessairement effectuées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du présent règlement* ».

Ce paragraphe indique clairement que les traitements pénaux réalisés par les autorités publiques relèvent de la seule directive, et que si ces autorités publiques mettent en œuvre des traitements à d’autres fins que pénales (mais qui relèvent du champ de l’Union), ces traitements relèvent du règlement.

1.1.1.2 Licéité du traitement

Aux termes de l’article 8 de la directive, le traitement de données à caractère personnel en matière pénale n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article premier de la directive, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.

Par ailleurs, une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement.

1.1.1.3 Principes généraux et conditions spécifiques applicables au traitement

Aux termes de l'article 4§1 de la directive, les données à caractère personnel doivent être :

- traitées de manière licite et loyale ;
- collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;
- exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

S'agissant des finalités du traitement, l'article 4§2 et §3 ainsi que l'article 9 de la directive précisent les règles applicables aux traitements initialement collectés pour l'une des finalités de la directive et ultérieurement effectués à d'autres fins.

L'article 4§2 de la directive prévoit ainsi que le traitement de données à caractère personnel pour une finalité relevant du champ d'application de la directive, autre que celles pour lesquelles les données ont été collectées, est autorisé à la double condition que conformément au droit de l'Union ou au droit national, le responsable du traitement soit autorisé à traiter ces données à caractère personnel pour une telle finalité, et que le traitement soit nécessaire et proportionné à cette autre finalité.

L'article 4§3 précise que ce traitement des données peut comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques aux fins énoncées à l'article premier, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

L'article 9 de la directive prévoit par principe que les données initialement collectées par les autorités compétentes pour une finalité relevant du champ d'application de la directive ne peuvent pas être traitées à d'autres fins, sauf exception prévue par le droit national ou le droit de l'Union.

L'article 9 précise que dans ce cas, autrement dit lorsque le traitement est effectué à d'autres fins que celles de la directive, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, le règlement (UE) 2016/679 s'applique, et ce même si l'autorité chargée du traitement est effectivement une autorité compétente au sens de la directive.

S’agissant des conditions spécifiques applicables au traitement, le paragraphe 3 de l’article 9 ajoute que, lorsque le droit de l'Union ou le droit d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données doit informer le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.

Les conditions spécifiques sont précisées au considérant 36 de la directive, aux termes duquel « *Ces conditions pourraient, par exemple, comprendre une interdiction de transmission ultérieure des données à caractère personnel à autrui, une interdiction d'utilisation desdites données à des fins autres que celles pour lesquelles elles ont été transmises au destinataire, ou une interdiction d'informer la personne concernée lorsque le droit à l'information est limité en l'absence d'autorisation préalable de l'autorité compétente qui transmet les données* ».

Selon la directive, cette obligation doit également « *s'appliquer aux transferts de données par l'autorité compétente qui transmet les données à des destinataires dans des pays tiers ou des organisations internationales* ». Ainsi, le paragraphe 4 de l’article 9 prévoit que « *l'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux services, organes et organismes établis en vertu du titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dont relève ladite autorité compétente* ».

Enfin, afin « *d’appliquer le principe d’exactitude des données* » visé au considérant 30, l’article 7 de la directive prévoit que les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

1.1.1.4 Règles particulières à certains traitements ou catégories de données

Les articles 10 et 11 de la directive fixent des règles particulières à certains traitements ou catégories de données.

L’article 10 traite des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le traitement de telles données peut ainsi être autorisé en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement:

- lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre ;pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique; ou

- lorsqu’il porte sur des données manifestement rendues publiques par la personne concernée.

L’article 11 prévoit que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit national auquel le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

Ces décisions ne sont pas fondées sur les catégories particulières de données à caractère personnel visées à l'article 10, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place.

Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 est interdit, conformément au droit de l'Union.

1.1.1.5 Règles applicables au traitement réalisé par un sous-traitant

En vertu des articles 22 et 23 de la directive, le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite que sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit national.

De manière générale, l’article 22 prévoit que le sous-traitant n'agit que sur instruction du responsable du traitement. Ainsi, si, en violation de la directive, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

Aux termes de cet article, le sous-traitant doit notamment :

- veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

- selon le choix du responsable du traitement, supprimer toutes les données à caractère personnel ou les renvoyer au responsable du traitement au terme de la prestation des services de traitement des données, et détruire les copies existantes, à moins que le droit de l’Union ou le droit national n’exige la conservation des données à caractère personnel.

Par ailleurs, le sous-traitant ne doit pas recruter un autre sous-traitant sans l’autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d’une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l’ajout ou le remplacement d’autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d’émettre des objections à l’encontre de ces changements.

1.1.1.6 Effectuer une analyse d'impact relative à la protection des données

Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, l'article 27 de la directive impose que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Cette analyse contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

L'article 28 de la directive prévoit, dans son premier paragraphe, que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer, soit lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; soit lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

Ce même article 28 impose, dans son paragraphe 4,que le responsable du traitement fournisse à l'autorité de contrôle l'analyse d'impact réalisée.

1.1.2 Conformité du droit national

1.1.2.1 Règles relatives au champ d'application de la directive et à la licéité du traitement

Les règles relatives au champ d'application de la directive et à la licéité du traitement, qui sont étroitement liées, devront faire l'objet d'une transposition.

1.1.2.2. Principes généraux et conditions spécifiques applicables au traitement

L'article 6 de loi informatique et libertés prévoit déjà qu'un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV

et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Par ailleurs, l'article 30 9° de loi impose que les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés lors de la création d'un traitement précisent les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant.

Enfin, en vertu de l'article 34 de la loi, le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Le droit français est donc conforme aux exigences fixées par l'article 4§1 de la directive.

En revanche, les dispositions des articles 4§2 et §3 et 9 de la directive relatives aux traitements ultérieurs et aux conditions spécifiques applicables au traitement devront être transposées.

De même, n'ayant pas d'équivalent dans notre législation actuelle, la distinction, exigée par l'article 7 de la directive, entre les données à caractère personnel fondées sur des faits et sur des appréciations personnelles devra faire l'objet d'une transposition.

S'agissant des règles particulières à certains traitements ou catégories de données, l'article 8 I de loi informatique et libertés prévoit l'interdiction de principe de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci, sauf exception. Ne sont pas soumis à cette interdiction certains traitements mentionnés au IV, notamment ceux qui sont justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26, autrement dit les fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté portant sur des données mentionnés au I de l'article 8.

Les règles nationales applicables aux traitements relevant du champ d'application de la directive ne sont donc pas conformes aux exigences de l'article 10 de la directive, qui devra être transposé.

S'agissant par ailleurs des décisions individuelles automatisées, l'article 10 de la loi précise qu'aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Il ajoute qu'aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Il prévoit enfin que ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.

Devra donc être transposé le dernier alinéa de l'article 11 de la directive relatif au profilage, qui n'a pas d'équivalent dans la LIL.

1.1.2.3 Règles applicables au traitement réalisé par un sous-traitant

Aux termes de l'article 35 de la loi informatique et libertés, les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Le droit national est donc partiellement conforme aux exigences fixées par les articles 22 et 23 de la directive. Devront notamment être transposés le fait que le sous-traitant doit être considéré comme un responsable du traitement s'il détermine, en violation de la directive, les finalités et les moyens du traitement ; les règles de recours à un autre sous-traitant et certaines obligations mise à la charge du sous-traitant.

1.1.2.4 Effectuer une analyse d'impact relative à la protection des données

N'ayant pas d'équivalent dans la loi informatique et libertés, l'exigence européenne d'effectuer dans certains cas une analyse d'impact relative à la protection des données devra faire l'objet d'une transposition.

1.2. CADRE CONSTITUTIONNEL

En matière de traitement de données, le Conseil constitutionnel est passé d'un contrôle limité à l'absence de disproportion manifeste à un contrôle de proportionnalité plus poussé.

Le Conseil constitutionnel a d'abord admis que les dispositions portant sur les traitements automatisés de données nominatives mis en œuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions, auxquels s'applique la loi du 6 janvier 1978, prévoient un ensemble de garanties « *de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée*». Il a par ailleurs jugé «*qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées*»[115].

Dans sa décision n° 2012-652 DC du 22 mars 2012, il a précisé ses exigences en matière de contrôle de fichiers en affirmant que «*la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif*»[116].

Dans l'exercice de ce contrôle de proportionnalité, le Conseil constitutionnel tient notamment compte du nombre de personnes susceptibles de relever du fichier informatique en cause, de la sensibilité particulière des données personnelles recueillies, des garanties techniques ou juridiques prévues par le législateur et des finalités d'utilisation ou de consultation du fichier.

1.3. CADRE CONVENTIONNEL

L'article 8 paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne prévoit que toute personne a le droit à la protection des données à caractère personnel la concernant, et que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi.

[115] Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, cons. 21 à 27 et 28 à 35.
[116] Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité, cons. 8 ; cf également décision n° 2016-745 DC du 26 janvier 2017, Loi relative à l'égalité et à la citoyenneté, paragr. 25

Dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, l'article 5 prévoit que « *les données à caractère personnel faisant l'objet d'un traitement automatisé sont:*

a) obtenues et traitées loyalement et licitement;
b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;
c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;
d) exactes et si nécessaire mises à jour;
e) *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées* ».

Son article 6 précise que « *les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales*. »

La Cour européenne des droits de l'homme attache une importance particulière à la protection des données à caractère personnel, qui joue selon elle un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention[117]. Ainsi juge-t-elle que le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8.

Selon la Cour, «*le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs, tout en offrant une possibilité concrète de présenter une requête en effacement des données mémorisées*[118]».

L'appréciation du caractère proportionné de la durée de conservation des données au regard du but poursuivi doit être faite en tenant compte de l'existence d'un contrôle indépendant de la justification de leur maintien dans le fichier, fondé sur des critères précis tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne, ou toute autre circonstance particulière[119].

---

[117] Examen de la conformité à l'article 8 des fichiers FIJAIS (CEDH, 17 décembre 2009, M.B. c. France, n° 22115/06), FAED (CEDH, 18 avril 2013, M.K. c. France, n° 19522/09), STIC (CEDH, 18 septembre 2014, Brunet c. France) et FNAEG (CEDH, 22 juin 2017)

[118] CEDH, 22 juin 2017, Aycaguer c.France, n° 8806/12, §38

[119] Dans son arrêt précité du 18 septembre 2014, la Cour a considéré que la durée de vingt ans de conservation des données inscrites au STIC était «*importante, compte tenu de l'absence de déclaration judiciaire de culpabilité et du classement sans suite de la procédure après le succès de la médiation pénale*» (§ 39 et 40).

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

2.1.1. Définir le champ d'application de la directive

L'article 19 insère, dans un chapitre unique, l'ensemble des règles applicables au traitement de données à caractère personnel en matière pénale prévues par la directive.

Ces règles fixées par les nouveaux articles 70-1 à 70-27 s'appliquent par dérogation aux autres dispositions de la loi actuelle.

Afin de délimiter le champ d'application de la directive, il est créé un nouvel article 70-1, qui prévoit ainsi que les dispositions du présent chapitre s'appliquent, le cas échéant par dérogation aux autres dispositions de la présente loi, aux traitements des données à caractère personnel mis en œuvre :

1° A des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

2° Par toute autorité publique compétente pour l'une des finalités énoncées au 1°, ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommée autorité compétente.

2.1.2. Respecter les exigences européennes liées à la licéité du traitement

Afin de mettre notre droit national en conformité avec l'article 8 de la directive, le troisième paragraphe de l'article 70-1 prévoit que les traitements relevant de la directive ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour les finalités énoncées au 1°, par une autorité compétente au sens du 2°, et où sont respectées les dispositions des articles 70-3 et 70-4.

L'option de maintenir les formalités préalables à la création d'un tel traitement, prévue par l'article 70-3, a en effet été retenue.

2.1.3 Mettre notre droit en conformité avec les règles particulières applicables aux traitements comportant des données sensibles

Afin de transposer l'article 10 de la directive, il est créé un nouvel article 70-2, qui prévoit que le traitement de données mentionnées au I de l'article 8 est uniquement possible en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et, soit s'il est prévu par un acte législatif ou règlementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.

Par ailleurs, les formalités préalables à la création d'un traitement portant sur des données mentionnées au I de l'article 8, à savoir un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, sont maintenus (cf infra).

2.1.4. Mettre notre droit en conformité avec l'exigence nouvelle d'une analyse d'impact relative à la protection des données à caractère personnel

Afin de respecter les articles 27 et 28 de la directive, l'article 70-4 prévoit que si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données sensibles, à savoir celles mentionnées au I de l'article 8, le responsable du traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.

Lorsque le traitement est effectué pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue par l'article 30 de la loi informatique et libertés compte tenu du maintien des formalités préalables à la création d'un tel traitement.

Dans les autres cas, lorsque le traitement entre dans le champ de la directive sans être effectué pour le compte de l'Etat, les troisième à cinquième alinéas de l'article 70-4 transposent l'article 28 §1 de la directive. Ils imposent ainsi au responsable du traitement ou au sous-traitant de consulter la Commission nationale de l'informatique et des libertés préalablement au traitement des données à caractère personnel :

- soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
- soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

Il a été décidé d'imposer la réalisation de cette étude d'impact lorsque le traitement porte sur des données mentionnées au I de l'article 8, le traitement de ces données sensibles présentant des risques élevés pour les libertés et les droits des personnes concernées.

Parmi les traitements entrant dans le champ de la directive mais non mis en œuvre pour le compte de l'Etat, peuvent être cités les traitements mis en œuvre par la SNCF et par la RATP pour les données à caractère personnel provenant de caméras individuelles fournies aux agents des services de sécurité interne, notamment pour le constat des infractions, qui sont par ailleurs susceptibles de faire apparaître directement ou indirectement des données sensibles au sens de l'article 8[120].

[120] Décret n° 2016-1862 du 23 décembre 2016.

2.1.5. Transposer les règles applicables aux traitements ultérieurs

Afin de mettre notre droit en conformité avec les articles 4 et 9 de la directive, sont créés les articles 70-5 à 70-7.

L'article 70-5 reprend strictement l'article 9 de la directive relatif aux conditions spécifiques applicables au traitement, et plus particulièrement aux règles applicables aux traitements ultérieurs à des fins ne relevant plus du champ d'application de la directive.

L'article 70-6 transpose l'article 4§2 et §3 de la directive relatif au traitement ultérieur à des fins demeurant dans le champ d'application de la directive.

L'article 70-7 régit plus spécifiquement la question des traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques .

2.1.6. Mettre notre droit en conformité avec l'obligation de distinguer les données à caractère personnel fondées sur des faits de celles fondées sur des appréciations personnelles

Afin de respecter l'article 7§1, il est créé un nouvel article 70-8 qui impose cette distinction entre les données à caractère personnel fondées sur des faits et celles fondées sur des appréciations personnelles.

2.1.7. Mettre notre droit en conformité avec les règles applicables aux décisions individuelles automatisées

Afin de mettre le système juridique français en conformité avec l'article 11 de la directive, l'article 70-9 prévoit, de manière combinée avec l'article 10 de la loi informatique et libertés relatif aux décisions individuelles prises sur le fondement d'un traitement automatisé de données personnelles, que tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 8 est interdit.

2.1.8. Mettre notre droit en conformité avec les règles applicables aux traitements effectués par un sous-traitant

Le nouvel article 70-10 transpose les exigences européennes fixées par les articles 22 et 23 de la directive.

Certaines de ces exigences étant strictement identiques à celles prévues par les paragraphes 1, 2, 9 et 10 de l'article 28 et l'article 29 du règlement (UE) 2016/679, un renvoi à ces dispositions est opéré.

Est en revanche directement transposé le paragraphe 3 de l'article 22 de la directive, compte tenu des différences existantes avec le règlement. L'article 70-10 prévoit ainsi que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du

responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement et qui prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement.

2.2 NECESSITE DE LEGIFERER

Outre les dispositions sur le champ d'application de la directive qui doivent être transposées, l'objectif du projet de loi est de mettre notre droit national en conformité avec les exigences énoncées par la directive, plus particulièrement avec :

- l'obligation nouvelle de réaliser, sous certaines conditions, une analyse d'impact relative à la protection des données,
- les règles relatives aux traitements de données effectués pour d'autres finalités que celles pour lesquelles elles avaient été collectées,
- la distinction entre les données personnelles fondées sur des faits et celles fondées sur des appréciations personnelles,
- les règles particulières relatives aux décisions individuelles automatisées,
- les règles applicables aux traitements effectués par un sous-traitant.

3. OPTIONS

3.1. Maintenir ou supprimer les formalités préalables à la création d'un traitement mis en œuvre pour le compte de l'Etat

3.1.1. Option 1 (écartée) : Supprimer les formalités préalables

De nombreux traitements relevant du champ d'application de la directive sont actuellement soumis à des formalités préalables contraignantes lors de leur création.

Ainsi, l'article 26 de la loi Informatique et Libertés du 6 janvier 1978 impose que la création du traitement mis en œuvre pour le compte de l'Etat qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ou qui a pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté, soit autorisée par un acte réglementaire, arrêté ou décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.

Or la directive n'impose pas aux Etats membres la création de telles formalités préalables pour la création d'un traitement de données entrant dans son champ d'application, sauf dans certains cas. Aux termes de l'article 28 de la directive, le responsable du traitement doit en effet uniquement consulter l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer, soit lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; soit lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

L'option permise par la directive de supprimer les formalités préalables a été écartée.

3.1.2. Option 2 (retenue) : Maintenir les formalités préalables

Les formalités préalables à la création d'un traitement mis en œuvre pour le compte de l'Etat en matière pénale représentent des garanties supplémentaires pour les droits des personnes concernées.

Pour ces raisons et afin d'éviter de remettre en cause un principe mis en œuvre depuis trente-huit ans, l'option retenue a été de les maintenir.

Cette option est en effet permise par l'article premier paragraphe 3 de la directive, qui autorise les Etats membres à prévoir des garanties plus étendues pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes, ainsi que par le considérant 15 de la directive qui prévoit notamment que « *le rapprochement des législations des États membres ne devrait pas conduire à un affaiblissement de la protection des données à caractère personnel qu'elles offrent mais devrait, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union. Il convient que les États membres ne soient pas empêchés de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes* ».

Ainsi, le nouvel article 70-3 prévoit que si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités prévues au 1° de l'article 70-1, il doit être prévu par un acte règlementaire pris conformément au I de l'article 26 et aux articles 28 à 31, soit par arrêté pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.

Si le traitement porte sur des données sensibles à savoir celles mentionnées au I de l'article 8, il est prévu par un acte règlementaire pris conformément au II de l'article 26, soit par un décret en Conseil d'Etat pris avis motivé et publié de la Commission nationale de l'informatique et des libertés.

3.2. Fixer des délais d'effacement ou de vérification régulière des données

3.2.1. Option 1 (écartée) : Ne pas prévoir de délais de conservation maximums mais imposer la vérification régulière de la nécessité de conserver les données

L'article 4 de la directive prévoit par principe que les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées, ce qui correspond à l'article 6 de la loi Informatique et libertés.

L'article 5 de la directive impose plus particulièrement aux Etats membres de prévoir des délais appropriés soit pour l'effacement des données, soit pour la vérification régulière de la nécessité de les conserver.

La directive ouvre donc une option permettant de ne pas prévoir de délai maximal de conservation, mais simplement de fixer des modalités pour le responsable du traitement de vérifier régulièrement s'il est toujours nécessaire de les conserver au regard des finalités du fichier.

Cette option n'a pas été retenue, car il paraît plus simple de toujours prévoir, comme actuellement, une durée maximale de conservation.

Cela n'interdit nullement, spécialement si cette durée maximale est particulièrement longue, de permettre des demandes d'effacement par anticipation, de telles possibilités pouvant du reste correspondre à des exigences conventionnelles et/ou constitutionnelles.

3.2.2. Option 2 (retenue) : Fixer des délais d'effacement des données

Le droit français fixe déjà, dans les textes applicables ou lors de la création du traitement, une durée maximale de conservation des données dans les fichiers.

Lors de la création d'un traitement, la demande d'avis adressée à la Commission nationale de l'informatique et des libertés doit en effet préciser la durée de conservation des informations traitées conformément à l'article 30 I. 5° de la loi Informatique et libertés.

Dans notre législation, et à titre d'illustration, les données ne peuvent être conservées dans le traitement des antécédents judiciaires (TAJ), destiné à faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, que pour une durée variant de 5 à 20 ans selon la gravité de l'infraction commise et l'âge de l'auteur aux termes de l'article R. 40-27 du code de procédure pénale.

De même, les données figurant au fichier national automatisé des empreintes génétiques (FNAEG), destiné à faciliter l'identification et la recherche des auteurs d'infraction, ne peuvent pas être conservées au-delà de 25 ans ou de 40 ans aux termes de l'article R. 53-14 du code de procédure pénale.

Les données inscrites au fichier automatisé des empreintes digitales (FAED), destiné à faciliter la recherche et l'identification des auteurs de crimes et de délits et de faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie, ne peuvent pas être conservées au-delà de 10 à 25 ans aux termes de l'article 5 du décret n°87-249 du 8 avril 1987.

L'option plus protectrice pour les droits et libertés de délais butoirs de conservation des données a donc été retenue.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

La présente disposition conduit à insérer dans la loi de 1978 dix nouveaux articles (articles 70-1 à 70-10).

DISPOSITIONS DU PROJET DE LOI	DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Article 19 PJL **Article 70-1 LIL**	Transposition des articles 1 et 2 (champ d'application), 3 (définitions) et 8 (licéité)
Article 70-2	Article 10
Article 70-3	Option permise par l'article 1§3 et le considérant 15 de la directive
Article 70-4	Articles 27 et 28
Article 70-5	Article 9
Articles 70-6 et 70-7	Article 4§2 et §3
Article 70-8	Article 7§1
Article 70-9	Article 11
Article 70-10	Transposition combinée des articles 22 et 23.

5. CONSULTATION ET MODALITÉS D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

La réforme s'appliquera le 25 mai 2018, conformément à l'article 24 du projet de loi.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précisera que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement, et qui prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement.

Les présentes dispositions du projet de loi seront applicables sur l'ensemble du territoire, hors les collectivités d'outre-mer soumises au principe de spécialité, pour lesquelles l'extension se fera par ordonnance.

ARTICLE 19 SECTION 2

OBLIGATIONS INCOMBANT AUX AUTORITES COMPETENTES ET AUX RESPONSABLES DE TRAITEMENT

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

1.1.1 Conformité du droit français à la directive sur les droits des personnes concernées par les données personnelles

1.1.1.1 Texte de la directive

La directive fixe des obligations aux autorités compétentes ainsi qu'aux responsables de traitement et aux sous-traitants.

1.1.1.1.1. Mettre à jour les données

Aux termes de son article 7 paragraphe 2, la directive impose aux autorités compétentes de prendre toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition.

À cette fin, chaque autorité compétente doit vérifier, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.

Lors de toute transmission de données à caractère personnel, doivent ainsi être ajoutées, dans la mesure du possible, des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour.

Le considérant 32 de la directive précise le champ d'application de cette obligation en ces termes : « *afin de garantir la protection des personnes physiques, l'exactitude, et la fiabilité des données à caractère personnel transmises ou mises à disposition ainsi que leur exhaustivité ou leur niveau de mise à jour, les autorités compétentes devraient, dans la mesure du possible, ajouter les informations nécessaires dans tous les transferts de données à caractère personnel* ».

Aux termes de l'article 7 paragraphe 3, s'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité

1.1.1.1.2. Opérer une distinction selon les catégories de personnes concernées

En vertu de son article 6, la directive impose au responsable du traitement d'établir, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées telles que :

- les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;
- les personnes reconnues coupables d'une infraction pénale ;
- les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;
- les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux deux premiers points.

1.1.1.1.3 Respecter des règles destinées à assurer la sécurité des données

1° Prendre des mesures techniques et organisationnelles appropriées

Aux termes de son considérant 53, la directive rappelle que la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées, qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut.

Ainsi, les articles 19 et 20 prévoient, à titre d'obligations générales, que le responsable du traitement doit, compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, mettre en œuvre les mesures techniques et organisationnelles appropriées, telles que la pseudonymisation :

- pour s'assurer et être en mesure de démontrer que le traitement est conforme aux exigences de la directive et à la protection des droits des personnes concernées,
- pour garantir que par défaut, seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement sont traitées, et que les données ne soient pas rendues accessibles à un nombre indéterminé de personnes sans l'intervention de la personne concernée.

Ces dispositions sont également applicables au sous-traitant.

L'article 22 prévoit en effet que le sous-traitant auquel le responsable du traitement fait appel doit présenter des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement soit conforme aux exigences de la directive et à la protection des droits des personnes concernées.

Le considérant 53 de la directive précise par ailleurs que « *le sous-traitant devrait tenir compte du principe de protection des données dès la conception et par défaut* ».

L’article 29 de la directive impose également au responsable du traitement et au sous-traitant de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Aux termes de son considérant 60, « *il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. […] Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient d'apprécier les risques que présente le traitement de données, tels que la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles, notamment, d'entraîner des dommages physiques, matériels ou un préjudice moral*».

Ainsi l’article 29 de la directive prévoit des dispositions spécifiques au traitement de données sensibles et aux traitements automatisés.

Son premier paragraphe impose ainsi au responsable du traitement et au sous-traitant de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Son second paragraphe fixe une liste de mesures à mettre en œuvre par le responsable du traitement ou le sous-traitant dans le cadre d’un traitement automatisé, à savoir :
a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations);
b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);
c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation);
d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);
e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données);
f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission);
g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);
i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration);
j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

2° Tenir un registre et un journal des activités et de certaines opérations de traitement et coopérer avec l'autorité de contrôle

Afin de pouvoir démontrer la licéité du traitement, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données tel que rappelé par les considérants 56 et 57, la directive impose deux obligations au responsable du traitement et au sous-traitant.

La première obligation fixée par l'article 24 de la directive est de tenir un registre écrit pour toutes les catégories d'activités de traitement relevant de leur responsabilité. Chaque responsable du traitement et sous-traitant devra être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de cette dernière sur sa demande pour qu'ils puissent servir au contrôle de ces opérations de traitement.

La seconde obligation prévue par l'article 25 de la directive est d'établir des journaux au moins pour les opérations de collecte, de modification, de consultation, de communication, y compris les transferts, l'interconnexion ou l'effacement, effectuées dans des systèmes de traitement automatisé.

Les journaux des opérations de consultation et de communication doivent permettre d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel.

Ces journaux ne doivent être utilisés qu'à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et pour les besoins de procédures pénales.

Afin de permettre à l'autorité de contrôle d'exercer pleinement son contrôle, le responsable du traitement et le sous-traitant sont tenus de lui mettre ces journaux à disposition sur demande.

De manière générale aux termes de l'article 26 de la directive, le responsable du traitement et le sous-traitant sont tenus de coopérer avec l'autorité de contrôle, à sa demande, dans l'exécution de ses missions.

3° Informer l'autorité de contrôle et la personne concernée en cas de violation de données à caractère personnel

En cas de violation de données à caractère personnel, les articles 30 et 31 de la directive fixent deux obligations d'information à la charge du responsable du traitement et destinées l'une à l'autorité de contrôle, l'autre à la personne concernée.

En premier lieu, le responsable du traitement doit notifier la violation à l'autorité de contrôle, à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et les libertés d'une personne physique. Il doit documenter toute violation en indiquant notamment les mesures prises pour y remédier, afin de permettre à l'autorité de contrôle de procéder aux vérifications nécessaires. Le sous-traitant doit également notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Enfin, lorsque la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre ou à celui-ci, les mêmes informations que celles imposées lors de la notification à l'autorité de contrôle doivent être communiquées au responsable du traitement de cet État membre dans les meilleurs délais.

En second lieu, le responsable du traitement doit, lorsque cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne physique, la communiquer à la personne concernée dans les meilleurs délais.

Par exception, il n'est pas tenu à cette obligation si :
- il a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces dernières ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;
- il a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et les libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;
- cette communication exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, soit exiger du responsable du traitement qu'il procède à cette communication, soit décider qu'il n'est effectivement pas tenu à cette obligation au vu des exceptions ci-dessus décrites.

La directive prévoit enfin que la communication à la personne concernée peut être retardée, limitée ou omise, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, protéger la sécurité publique, protéger la sécurité nationale ou protéger les droits et libertés d'autrui.

1.1.1.4. Désigner un délégué à la protection des données

L'article 32 impose au responsable du traitement de désigner un délégué à la protection des données, excepté pour les autorités judiciaires agissant dans l'exercice de leur fonction juridictionnelle.

Les articles 33 et 34 de la directive détaillent les fonctions et les missions de ce délégué qui comprennent notamment celles d'informer et de conseiller le responsable du traitement et de contrôler le respect de la directive.

1.1.1.2. Conformité du droit national

1.1.1.2.1. Sur l'obligation de mise à jour des données incombant aux autorités compétentes

L'actuelle loi informatique et libertés ne fixe pas d'obligation pour les autorités compétentes de veiller à la qualité des données transmises.

Cette obligation nouvelle fixée par l'article 7 de la directive devra donc faire l'objet d'une transposition en droit national.

1.1.1.2.2 Sur les obligations incombant aux responsables de traitement et sous-traitants

1° Sur la distinction entre les différentes catégories de personnes concernées

Le droit français opère déjà des distinctions selon les différentes catégories de personnes concernées.

A titre d'illustration, les conditions d'inscription dans le traitement, les durées de conservations et les conditions d'effacement des données sont modulées dans le traitement des antécédents judiciaires (TAJ), dans le FNAEG et dans le FAED, selon que la personne concernée est une victime, un mis en cause majeur ou mineur.

Néanmoins, notre législation n'impose pas de manière générale au responsable du traitement d'opérer une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées.

Les dispositions de l'article 6 de la directive devront donc être transposées.

2° Sur les règles destinées à assurer la sécurité des données personnelles

S'agissant des règles destinées à assurer l'intégrité et la sécurité des données personnelles, les mesures prises par le responsable de traitement font l'objet d'un examen lors des formalités préalables à la création.

L'article 30 de la loi informatique et libertés prévoit en effet au titre de son 9° que les demandes d'avis adressées à la Commission nationale de l'informatique et des libertés doivent notamment

préciser « *les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi* ». La Commission opère donc un contrôle de la sécurité du traitement au stade de sa création.

Par ailleurs, l'article 34 de la loi impose de manière générale au responsable du traitement de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

La loi modifiée du 6 janvier 1978 impose donc aux responsables de traitement une obligation de sécurité et de confidentialité.

Cette obligation n'apparait néanmoins pas suffisante au regard des exigences européennes, et plus particulièrement à l'aune de la nécessité d'une protection des données par défaut, d'une obligation de sécurité renforcée pour toutes les données sensibles visées à l'article 8 et de la liste des mesures à mettre en œuvre dans le cadre d'un traitement automatisé.

Les articles 19, 20 et 29 de la directive devront donc faire l'objet d'une transposition.

3° Sur l'obligation de tenue d'un registre et d'un journal

N'ayant pas d'équivalent dans la loi informatique et libertés, les obligations nouvelles pour le responsable du traitement et pour le sous-traitant de tenir un registre de toutes les activités de traitement effectuées, ainsi qu'un journal de certaines opérations effectuées dans des systèmes de traitement automatisé afin de pouvoir démontrer la licéité du traitement et de garantir l'intégrité et la sécurité des données, devront faire l'objet d'une transposition.

4° Sur les obligations d'information en cas de violation de données à caractère personnel

L'article 34 bis de la loi modifiée du 6 janvier 1978 issu de l'ordonnance n° 2011-1012 du 24 août 2011 fixe les règles à suivre en cas de violation de données à caractère personnel.

Ces règles ne concernent cependant pas toutes les hypothèses de violation. Elles sont en effet limitées aux violations de données à caractère personnel intervenant dans des traitements des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.

En pratique, sont dès lors uniquement soumis à l'article 34 bis de la loi modifiée du 6 janvier 1978 les fournisseurs d'accès à l'Internet et les opérateurs de téléphonie mobile.

Les exigences européennes fixées par les articles 30 et 31 de la directive en cas de violation de données à caractère personnel étant applicables à tous les traitements, elles devront donc être transposées en droit national.

5° Sur l'obligation de désigner un délégué à la protection des données

L'article 22 III de la loi informatique et libertés et les articles 42 à 56 du décret du 20 octobre 2005 prévoient la possibilité pour le responsable du traitement de désigner un correspondant à la protection des données.

Par cette désignation facultative, le droit français n'est donc pas conforme aux exigences européennes qui prévoient la désignation obligatoire du délégué.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision n° 2004-499 DC du 29 juillet 2004 portant sur la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le Conseil constitutionnel a conclu que le fait, par la création d'un correspondant à la protection des données, de dispenser le responsable du traitement de certaines formalités préalables sauf exception était conforme à la Constitution.

Le Conseil a notamment considéré que compte tenu de l'ensemble des précautions prises, s'agissant en particulier de la qualification, du rôle et de l'indépendance du correspondant, la dispense de déclaration résultant de sa désignation ne privait de garanties légales aucune exigence constitutionnelle[121].

1.3. CADRE CONVENTIONNEL

L'article 8 paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne prévoit que toute personne a le droit à la protection des données à caractère personnel la concernant, et que le respect de cette règle est soumis au contrôle d'une autorité indépendante.

Aux termes de l'article 7 de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, des « *mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés* ».

[121] Décision n° 2004-499 DC du 29 juillet 2004, cons. 21 à 23

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

2.2.1. Mettre notre droit en conformité avec l'obligation de veiller à la fiabilité des données personnelles transmises ou mises à disposition

Afin de respecter l'article 7 paragraphe 2 de la directive, il est créé un nouvel article 70-11 qui reprend strictement les exigences européennes, et plus particulièrement l'obligation nouvelle pour les autorités compétentes de prendre toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition.

Le dernier alinéa de l'article 70-11 transpose l'article 7 paragraphe 3 de la directive, et prévoit ainsi que le destinataire est informé sans retard en cas de transmission de données personnelles inexactes ou de transmission illicite, et que les données sont alors rectifiées ou effacées ou leur traitement limité.

2.2.2. Mettre notre droit en conformité avec la nécessité pour le responsable du traitement d'établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées

Pour mettre notre droit en conformité avec l'article 6 de la directive qui impose de distinguer les données personnelles selon des catégories de personnes concernées, il est créé un article 70-12.

Cet article reprend intégralement les dispositions de la directive et impose ainsi au responsable du traitement de distinguer entre les données à caractère personnel des catégories suivantes de personnes concernées :

1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;

2° Les personnes reconnues coupables d'une infraction pénale;

3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale; et

4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux 1° et 2°.

2.2.3. Mettre notre droit en conformité avec les obligations imposées au responsable du traitement et au sous-traitant en vue de garantir l'intégrité et la sécurité des données

Pour plus de lisibilité, a été retenue l'option, au sein du nouvel article 70-13, d'une transposition combinée des articles 19, 20 et 29 de la directive, qui imposent au responsable du traitement et au sous-traitant de garantir l'intégrité et la sécurité des données.

Les dispositions figurant dans les articles 19, 20 et 29§1 de la directive étant identiques à celles prévues par les paragraphes 1 et 2 des articles 24 et 25 du règlement, un renvoi à ces articles du règlement est opéré dans l'article 70-13.

L'article 70-13 transpose par ailleurs les dispositions de la directive qui n'ont pas d'équivalent ni dans la loi informatique et libertés ni dans le règlement.

Ainsi, le nouvel article 70-13 ajoute que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin degarantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8.

En ce qui concerne le traitement automatisé, l'article 70-13 reprend intégralement la liste des mesures devant être mises en œuvre par le responsable du traitement et le sous-traitant aux termes de l'article 29§2 de la directive.

2.2.4. Mettre notre droit en conformité avec les obligations nouvelles pour le responsable du traitement et le sous-traitant de tenir un registre des activités de traitement effectuées, ainsi qu'un journal de certaines opérations

Afin de respecter les exigences européennes fixées par l'article 24 de la directive, il est créé un nouvel article 70-14 qui prévoit que le responsable du traitement et son sous-traitant tiennent un registre des activités de traitement, et le mettent à la disposition de la Commission nationale de l'informatique et des libertés sur demande.

Les conditions dans lesquelles ce registre doit être tenu sont prévues de manière similaire par l'article 24 de la directive et les paragraphes 1 à 4 de l'article 30 du règlement.

Dès lors, le nouvel article 70-14 opère un renvoi aux paragraphes 1 à 4 de l'article 30 du règlement, et ne réécrit que les dispositions propres à la directive, soit la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.

Le nouvel article 70-15 prévoit, conformément à l'article 25 de la directive, que le responsable du traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation, de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données.

Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et leurs destinataires.

Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales. Il est mis à disposition de la Commission nationale de l'informatique et des libertés à sa demande.

Enfin, de manière générale, le nouvel article 70-16 impose au responsable de traitement et au sous-traitant, par le renvoi à l'article 31 du règlement qui est identique à l'article 26 de la directive, de coopérer avec la Commission nationale de l'informatique et des libertés à la demande de celle-ci dans l'exécution de ses missions.

2.2.5. Mettre notre droit en conformité avec les règles fixées en cas de violation de données à caractère personnel

Afin de respecter les exigences européennes en cas de violation de données personnelles dans tout type de traitement relevant du champ d'application de la directive, l'article 70-16 transpose les deux obligations d'information mises à la charge du responsable du traitement par les articles 30 et 31 de la directive : la notification de la violation à la Commission nationale de l'informatique et des libertés et la communication de la violation à la personne concernée.

Les articles 30 et 31 de la directive étant identiques aux articles 33 et 34 du règlement, excepté le paragraphe 6 de l'article 30 et le paragraphe 5 de l'article 31, l'article 70-16 opère un renvoi à ces dispositions du règlement.

Les dispositions propres des paragraphe 6 de l'article 30 et paragraphe 5 de l'article 31de la directive sont, quant à elles, reproduites aux deuxième et troisième alinéas de l'article 70-16, qui prévoit ainsi que :

- le responsable du traitement notifie également la violation au responsable du traitement de l'autre Etat membre dans les meilleurs délais si cette violation porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre Etat membre ou à celui-ci,
- la communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée aussi longtemps qu'une telle mesure est nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour ne pas mettre en danger la sécurité publique, la sécurité nationale ou les droits ou libertés d'autrui ou ne pas faire obstacle au bon déroulement des enquêtes et procédures destinées à prévenir, détecter ou poursuivre des infractions pénales ou à

exécuter des sanctions pénales.

2.2.6. Mettre notre droit en conformité avec l'obligation de désigner un délégué à la protection des données

A cette fin, il est créé un article 70-17 qui transpose les articles 32 à 34 de la directive.

Cet article renvoie aux dispositions des paragraphes 5 et 7 de l'article 37, des paragraphes 1 et 2 de l'article 38 et du paragraphe 1 de l'article 39 du règlement qui sont identiques à celles de la directive, à une exception près. Contrairement à la directive qui n'impose les obligations relatives au délégué à la protection des données qu'au responsable du traitement, certaines dispositions du règlement les font également peser sur le sous-traitant. L'article 70-15 prévoit dès lors que ce renvoi au règlement ne concerne que le responsable de traitement.

L'article 70-15 reprend par ailleurs littéralement l'article 32§3 de la directive, qui n'a pas d'équivalent dans le règlement, en prévoyant qu'un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille.

2.2 NECESSITE DE LEGIFERER

L'objectif immédiat du projet de loi est de mettre notre droit national en conformité avec les exigences énoncées par la directive, plus particulièrement avec l'obligation nouvelle pour les autorités compétentes de veiller à la fiabilité des données personnelles transmises ou mises à disposition ; ainsi que pour le responsable du traitement, et également dans certains cas pour le sous-traitant :

- d'établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées,

- de prendre des mesures appropriées en vue de garantir l'intégrité et la sécurité des données,

- de tenir un registre des activités de traitement effectuées, et un journal de certaines opérations effectuées dans des systèmes de traitement automatisé,

- d'informer l'autorité de contrôle et la personne concernée en cas de violation de données à caractère personnel dans tout traitement,

- de désigner un délégué à la protection des données.

3. OPTIONS

3.1. Dispenser ou non les tribunaux et autorités judiciaires indépendantes de l'obligation de désigner un délégué à la protection des données dans l'exercice de leurs fonctions juridictionnelles

3.1.1. Option 1 (écartée) : Imposer la désignation d'un délégué à la protection des données aux tribunaux et autorités judiciaires indépendantes agissant dans l'exercice de leurs fonctions juridictionnelles

L'article 32 paragraphe 1 de la directive laisse à la libre appréciation des Etats membres la faculté de dispenser les tribunaux et d'autres autorités judiciaires indépendantes de l'obligation de désigner un délégué à la protection des données lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle.

Cette faculté est rappelée par le considérant 63 de la directive, qui précise que « *le responsable du traitement devrait désigner une personne qui l'aiderait à vérifier le respect, au niveau interne, des dispositions adoptées en vertu de la présente directive, sauf lorsqu'un État membre décide que des tribunaux et d'autres autorités judiciaires indépendantes en sont dispensés dans l'exercice de leur fonction juridictionnelle* ».

Cette option a été écartée.

3.1.2. Option 2 (retenue) : Les dispenser de désigner un délégué à la protection des données

S'agissant de traitements mis en œuvre par des autorités judiciaires dans l'exercice de leurs fonctions, l'option de ne pas leur imposer la désignation d'un délégué à la protection des données a été retenue.

3.2. Reporter ou non l'obligation de journalisation

Comme indiqué dans la partie relative à l'entrée en vigueur, il a été décidé de permettre un report de cette obligation, ce que permet l'article 63 de la directive.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1 IMPACTS JURIDIQUES

La présente disposition conduit à devoir insérer dans la loi de 1978 de nouveaux articles (articles 70-11 à 70-17).

DISPOSITIONS DU PROJET DE LOI	DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Article 70-11	Transposition des articles 4 (« sans tarder ») et 7§2 et §3
Article 70-12	Article 6
Article 70-130	Transposition combinée des articles 19, 20, 22§1 et 29
Article 70-14	Article 24
Article 70-15	Article 25
Article 70-16	Transposition combinée des articles 30 et 31
Article 70-17	Transposition combinée des articles 32 à 34

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES ET AUTRES TRAITEMENTS EXISTANTS

S'agissant notamment de l'obligation de journalisation prévue par l'article 25 de la directive et reprise par le nouvel article 70-15 il peut être fait les observations suivantes.

Actuellement, la loi "Informatique et Libertés" n'a pas de disposition spécifique concernant cette traçabilité. Toutefois l'article 34 de la loi fait peser sur les responsables de traitement des obligations de sécurité:

Cet article prévoit en effet que "*Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès*".

La CNIL est particulièrement attentive à la mise en œuvre de telles mesures de traçabilité, dans la mesure où cela permet de détecter notamment les détournements de finalité et de s'assurer, a posteriori, que seules les personnes ayant besoin d'en connaître ont eu accès aux données. D'ailleurs, sur certains traitements particulièrement sensibles (Cassiopée notamment), elle a même recommandé (Délibération n°2011-233 du 21 juillet 2011) la mise en place d'un mécanisme de remontée d'alerte (outil de détection des usages anormaux).

C'est en application de cet article 34 que le ministère de la justice, pour l'ensemble de ses traitements (ou à tout le moins pour les plus récents), met déjà en œuvre des mesures de traçabilité, qui permettent d'assurer la sécurité des données. Le plus souvent (notamment pour les traitements relevant de l'article 26 de la loi "Informatique et Libertés"), ces traces sont conservées par le ministère de la justice pendant 3 ans (durée beaucoup plus longue que dans le secteur privé). Dans la mesure où cette durée correspondait jusqu'à récemment à la durée de prescription de l'infraction de détournement de finalité, prévue à l'article 226-21 du code pénal, la Commission considérait que cette durée ne soulevait pas de difficulté.

Par ailleurs, les actes réglementaires entourant la mise en œuvre des traitements mentionnent le plus souvent expressément ces mesures de traçabilité (alors même que cela n'est pas une obligation au titre de l'article 29 de la loi). On peut citer comme exemple :

- Cassiopée: article R. 15-33-66-13 du CPP
- Genesis: article R. 57-9-26 du CPP

Toutefois, l'article 25 de la directive, comme le nouvel article 70-15, est précis, en ce sens qu'il décrit limitativement les fins pour lesquelles ces traces pourront être utilisées (vérification de la licéité du traitement, autocontrôle, garantie de l'intégrité et de la sécurité des données, procédure pénale), ce qui n'est pas le cas de la loi "Informatique et Libertés";

Or, actuellement, si les créations, modifications, suppressions et les consultations de données sont les actions le plus souvent tracées, il n'est pas sûr que la communication et l'interconnexion le soient systématiquement. Ce point nécessitera donc une confirmation des services compétents en la matière, afin que ces derniers précisent quelles sont les actions qui sont tracées, les traces générées et les éventuelles modifications informatiques à prévoir afin de s'assurer du respect de l'article 70-15 (il en va de même pour la mise en œuvre de telles mesures sur les applicatifs les plus anciens, qui pourraient éventuellement soulever des difficultés), afin de déterminer dans quelle mesure la possibilité de report doit être retenue pour tels ou tels fichiers.

Cette question concerne également les traitements relevant du ministère de l'intérieur ou d'autres ministères.

5. CONSULTATION ET MODALITÉS D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

La réforme s'appliquera le 25 mai 2018, conformément à l'article 24 du projet de loi.

Ces dispositions seront applicables sur l'ensemble du territoire, hors les collectivités d'outre-mer soumises au principe de spécialité, pour lesquelles l'extension se fera par ordonnance.

ARTICLE 18 ET ARTICLE 19 SECTION 3

DROITS DE LA PERSONNE CONCERNEE

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1 Conformité du droit français à la directive sur les droits des personnes concernées par les données personnelles

1.1.1 Texte de la directive

Le chapitre III de la directive fixe les règles applicables aux droits des personnes concernées par les données personnelles.

Par principe, l'article 12 de la directive impose au responsable du traitement de fournir à la personne concernée diverses informations, de procéder à toute communication nécessaire lorsque cette dernière lui demande l'accès ou la rectification des données la concernant, et de prendre toutes les mesures nécessaires pour faciliter l'exercice de ses droits par la personne concernée.

1.1.1.1 Dispositions spécifiques sur la portée des droits de la personne concernée

Les articles 13 à 17 de la directive traitent du droit de la personne concernée par les données, à disposer de certaines informations, à accéder, rectifier ou effacer du traitement les données personnelles la concernant, ainsi que de la limitation du traitement.

1° Droit à l'information

L'article 13 de la directive impose au responsable du traitement de mettre certaines informations à la disposition de la personne concernée.

Cet article consacre ainsi un droit à l'information pour la personne concernée en matière pénale.

Selon le premier paragraphe de l'article 13, ces informations doivent au moins préciser :

- l'identité et les coordonnées du responsable du traitement
- le cas échéant, les coordonnées du délégué à la protection des données;
- les finalités du traitement auquel sont destinées les données à caractère personnel;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de ladite autorité;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.

Selon le second paragraphe, le responsable du traitement doit également, dans des cas particuliers, fournir d'autres informations à la personne concernée afin de lui permettre d'exercer ses droits, à savoir :

- la base juridique du traitement,

- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales;
- au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

Le considérant 42 de la directive prévoit ainsi que « *dans des cas précis et afin de permettre à la personne concernée d'exercer ses droits, celle-ci devrait être informée de la base juridique du traitement et de la durée pendant laquelle les données seront conservées, dans la mesure où ces informations complémentaires sont nécessaires pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données sont traitées* ».

Ce principe d'un droit à l'information de la personne concernée peut néanmoins souffrir de certaines restrictions.

Ainsi le troisième paragraphe de l'article 13 de la directive permet aux Etats membres d'adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée en application du second paragraphe, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:
- éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
- éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;
- protéger la sécurité publique;
- protéger la sécurité nationale;
- protéger les droits et libertés d'autrui.

Le quatrième paragraphe de l'article 13 de la directive laisse à la libre appréciation des Etats membres la possibilité de déterminer des catégories de traitement susceptibles de relever des finalités susvisées.

2° Droit d'accès

Les règles relatives au droit d'accès de la personne concernée sont fixées par les articles 14 et 15 de la directive : l'article 14 pose le principe de ce droit, et l'article 15 délimite les restrictions pouvant y être apportées.

Aux termes de l'article 14 de la directive, la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes:

- les finalités du traitement ainsi que sa base juridique;
- les catégories de données à caractère personnel concernées;

- les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;
- la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée;
- le droit d'introduire une réclamation auprès de l'autorité de contrôle et les coordonnées de ladite autorité;
- la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.

Ce droit d'accès de la personne concernée à ses données personnelles peut néanmoins souffrir de certaines restrictions.

Le premier paragraphe de l'article 15 de la directive permet ainsi aux Etats membres de limiter, entièrement ou partiellement, ce droit dès lors que cette mesure est, de la même façon que pour le droit à l'information, nécessaire et proportionnée pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes, recherches, procédures, poursuites ou à l'exécution de sanctions pénales ou pour protéger la sécurité publique, nationale ou les droits et libertés d'autrui.

Le second paragraphe de l'article 15 ouvre une autre option aux Etats membres, en leur permettant de déterminer des catégories de traitement susceptibles de relever des finalités susvisées.

En cas de refus ou de limitation d'accès, la directive impose alors au responsable du traitement d'en informer la personne concernée dans les meilleurs délais, y compris en précisant les motifs de cette restriction.

Cette information de la personne concernée en cas de restriction de son droit d'accès par le responsable du traitement peut néanmoins ne pas être fournie lorsqu'elle risque de compromettre l'un des objectifs susvisés, liés à la protection de la sécurité ou des droits et libertés d'autrui ou à la prévention ou à la détection d'infractions pénales, aux enquêtes, recherches, procédures, poursuites ou à l'exécution de sanctions pénales.

Le responsable du traitement doit alors informer la personne concernée de son droit d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel. Il doit également consigner les motifs de fait ou de droit qui fondent sa décision, et mettre ces informations à la disposition des autorités de contrôle.

3° Droit de rectification ou d'effacement, et limitation du traitement

Par principe, aux termes du premier paragraphe de l'article 16 de la directive, la personne concernée a le droit, dans les meilleurs délais, d'obtenir du responsable du traitement que les données inexactes ou incomplètes la concernant soient rectifiées ou complétées.

Dans le second paragraphe de l'article 16, la directive complète ce droit de rectification par le droit pour la personne concernée d'obtenir du responsable du traitement l'effacement de certaines données dans les meilleurs délais. Ce droit à l'effacement existe lorsque le traitement ne respecte pas les dispositions des articles 4, 8 ou 10 de la directive autrement dit lorsqu'il ne respecte pas les principes généraux applicables aux traitements tels que ceux de licéité, de sécurité, de compatibilité avec les finalités légitimes pour lesquelles les données ont été collectées, de conservation pendant une durée adaptée, ou lorsqu'il porte sur des données inexactes ou, hors les cas prévus par la loi, sur des données dites sensibles ou enfin lorsqu'une obligation légale l'exige.

Au lieu d'effacer les données, la directive prévoit que le responsable du traitement peut limiter le traitement soit lorsqu'il ne peut pas être déterminé si les données sont ou non inexactes, soit lorsque ces données doivent être conservées à des fins probatoires.

Lorsque le responsable du traitement fait droit à la demande de rectification, il doit en informer l'autorité compétente dont les données proviennent, ainsi que le destinataire de ces données, à charge pour ce dernier de les rectifier sous sa responsabilité.

Lorsque le responsable du traitement fait droit à la demande d'effacement ou limite le traitement, il doit aviser le destinataire de ces données à charge pour lui de les effacer ou d'en limiter le traitement sous sa responsabilité.

Lorsque le responsable du traitement refuse de rectifier, d'effacer les données ou de limiter leur traitement, il doit en informer la personne concernée, en lui précisant les motifs ayant fondé sa décision. Néanmoins, la directive permet aux Etats membres de ne pas obliger le responsable du traitement à fournir ces informations lorsqu'à l'instar des restrictions possibles pour les droits à l'information et d'accès, cette mesure est nécessaire et proportionnée pour éviter de nuire à la prévention ou à la détection d'infractions pénales ou pour protéger la sécurité et les droits et libertés d'autrui.

En cas de refus, le responsable du traitement doit alors informer la personne concernée de son droit d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

1.1.1.2 Dispositions générales relatives aux modalités d'exercice des droits et de transmission des informations

1° Principe d'un exercice direct des droits par la personne concernée, doublé d'un exercice indirect en cas de restriction

Pour exercer ses droits d'information, d'accès et de rectification, d'effacement des données ou de limitation du traitement, la personne concernée s'adresse directement au responsable du traitement sans passer par l'intermédiaire d'une quelconque autorité.

Néanmoins, dans les cas visés par l'article 13 paragraphe 3, l'article 15 et l'article 16 paragraphe 4, autrement dit en cas de restriction des droits justifiées par la nécessité de ne pas nuire à la prévention ou à la détection d'infractions pénales et de protéger la sécurité et les droits et libertés

d'autrui, l'article 17 de la directive impose que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle.

Afin de permettre à la personne concernée d'exercer pleinement son droit par l'intermédiaire de l'autorité de contrôle, la directive impose alors au responsable du traitement de l'aviser de cette possibilité.

Aux termes de la directive, l'autorité de contrôle doit a minima informer la personne concernée qu'elle a procédé à toutes les vérifications nécessaires ou à un examen, et l'aviser de son droit de former un recours juridictionnel.

2° Principe d'une transmission claire et gratuite des informations à la personne concernée

En cas de doute raisonnable sur l'identité du demandeur, le responsable du traitement peut solliciter des informations complémentaires destinées à la confirmer.

Une fois cette identité confirmée, l'article 12 de la directive impose au responsable du traitement de fournir dans les meilleurs délais à la personne concernée les informations relevant de ses différents droits d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples, et ce sans exiger le moindre paiement.

Néanmoins dès lors que la demande adressée par une personne concernée est manifestement infondée ou excessive, notamment en raison de son caractère répétitif avec d'autres précédentes requêtes, le responsable du traitement est en droit soit d'exiger le paiement de frais raisonnables pour y répondre, soit de refuser d'y donner suite.

Le responsable du traitement dispose donc d'un pouvoir d'appréciation du bien-fondé des demandes, à charge pour lui néanmoins de rapporter la preuve du caractère manifestement infondé ou abusif de la demande en cas de contestation.

1.1.2 Conformité partielle du droit national

1.1.2.1 Dispositions spécifiques à chaque droit de la personne concernée

1° Absence de droit à l'information en matière pénale

L'article 32 de la loi Informatique et Libertés fixe les informations devant être mis à disposition de la personne concernée par le responsable de traitement. Cet article n'est néanmoins pas applicable, aux termes de son VI, « *aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales* ».

En outre, il fait partie dans la loi informatique et libertés de la section relative aux obligations incombant aux responsables de traitements, alors que dans la directive ces informations sont conçues comme faisant partie des droits de la personne concernée.

Devra donc être intégralement transposé l'article 13 de la directive qui crée un droit à l'information de la personne concernée en matière pénale.

2° Droit d'accès

La loi « informatique et libertés » permet déjà aux personnes concernées d'accéder aux données personnelles les concernant.

L'article 39 de la loi modifiée du 6 janvier 1978 prévoit ainsi que toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

- la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement;
- des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;
- le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
- la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
- les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

Le droit français est donc partiellement conforme à la directive en matière d'accès. Il est conforme quant au droit de la personne concernée d'obtenir la confirmation que les données la concernant sont ou ne sont pas traitées, ainsi que les informations relatives à la finalité du traitement, aux catégories de données, aux destinataires et à l'origine de l'information.

En revanche, devront être transposées les dispositions de la directive autorisant l'accès de la personne concernée aux autres informations, notamment à la base juridique du traitement, à la durée de conservation des données, à ses droits de demander la rectification, l'effacement ou la limitation du traitement et d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés.

Lorsqu'il est fait droit à la demande d'accès, la délivrance d'une copie des données peut être subordonnée au paiement par la personne concernée d'une somme qui ne peut excéder le coût de la reproduction.

Aux termes des articles 39 de la loi, 86 et 94 du décret, les demandes manifestement abusives peuvent être rejetées.

Afin de mettre en conformité le droit français avec la directive, des dispositions garantissant la gratuité des informations transmises dans le cadre du droit d'accès, sauf demande manifestement abusive ou infondée, devront donc être adoptées.

Dans notre législation, le droit d'accès peut s'exercer directement auprès du responsable pour la plupart des traitements, excepté pour certains traitements pour lesquels un régime dérogatoire

d'exercice indirect par l'intermédiaire de la Commission nationale de l'informatique et des libertés est prévu par la loi.

Ainsi, l'article 41 de la loi prévoit que la personne concernée ne peut exercer son droit d'accès que de manière indirecte lorsque ses données personnelles font l'objet d'un traitement qui *"intéresse la sûreté de l'État, la défense ou la sécurité publique"*.

Ces dispositions de l'article 41 sont également applicables, en vertu de l'article 42 de la loi, aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'un service public qui ont pour mission de prévenir, rechercher ou constater des infractions, si un tel droit est prévu dans l'acte autorisant la mise en œuvre du traitement.

A titre d'illustration, sont soumis à un régime de droit d'accès direct les traitements suivants:

- APPI, traitement mis en œuvre par les SPIP,
- AGRASC, traitement mis en œuvre par l'Agence de gestion et de recouvrement des avoirs saisis et confisqués aux fins de gestion et du recouvrement des biens saisis et confisqués,
- PSEM, traitement mis en œuvre par l'administration pénitentiaire aux fins de gestion des placements sous surveillance électronique mobile,
- GAME 2010, traitement de « gestion de l'activité et des mesures éducatives 2010 » mis en œuvre par la protection judiciaire de la jeunesse pour le suivi des mineurs,
- Cassiopée, traitement mis en œuvre dans les juridictions.

Toujours à titre d'illustration, sont notamment soumis à un régime de droit d'accès indirect :

- le TAJ, traitement des antécédents judiciaires,
- le FNIS, fichier national des interdits de stade,
- les fichiers EASP (enquêtes administratives relatives à la sécurité publique) et PASP (prévention des atteintes à la sécurité publique) des services de renseignement territorial,
- le SALVAC, système d'analyse et de liens de la violence associée aux crimes,
- ANACRIM, logiciel d'analyse criminelle.

Constituent des fichiers mixtes relevant d'un régime d'accès tantôt direct, tantôt indirect, le fichier des personnes recherchées (FPR), le système d'information Schengen (SIS) ou le traitement GENESIS mis en œuvre dans les établissements pénitentiaires.

Dans le cadre des traitements soumis à un régime de droit d'accès indirect, le droit national confère donc un rôle central à la Commission nationale de l'informatique et des libertés, puisque c'est à elle que doivent être transmises les demandes d'accès.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données ne met pas en cause les finalités du traitement ou la sûreté de l'Etat, la défense ou la sécurité publique, les informations peuvent être communiquées au requérant. En cas d'opposition du responsable de traitement, la commission doit simplement informer le requérant qu'il a été procédé aux vérifications nécessaires.

Devront donc être transposées en droit national les dispositions consacrant, pour tous les traitements relevant de son champ d'application y compris ceux de police judiciaire et intéressant la sécurité publique, le principe d'un droit d'accès direct de la personne concernée auprès du responsable du traitement, la possibilité d'un exercice indirect de ses droits n'étant maintenue qu'en cas de restriction de ses droits.

3° Droit de rectification ou d'effacement

L'article 40 de la loi informatique et libertés permet à toute personne physique justifiant de son identité d'exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données inexactes, incomplètes, équivoques, périmées la concernant ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le responsable du traitement doit alors pouvoir justifier, sans frais pour le demandeur, qu'il a procédé aux opérations nécessaires.

En cas de rectification ou d'effacement d'une donnée inexacte, incomplète, équivoque ou périmée auparavant transmise à un tiers, le responsable du traitement doit lui notifier les opérations effectuées.

A l'instar des règles applicables au droit d'accès, ce droit de rectification ou d'effacement s'exerce de manière directe, hors les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique et les traitements de police judiciaire prévus par les articles 41 et 42 de la loi.

Toute demande manifestement abusive peut être rejetée, aux termes des articles 86 et 94 du décret.

Le droit français est donc conforme pour ce qui concerne les possibilités offertes à la personne concernée de solliciter la rectification et la suppression de données personnelles, et d'obtenir gratuitement la réalisation et la communication de ces opérations.

Il ne prévoit en revanche aucune possibilité de limitation du traitement par le responsable.

Des dispositions devront par conséquent être adoptées en ce sens afin de respecter la directive.

Devront également être transposées les dispositions de la directive consacrant :

- pour tous les traitements relevant de son champ d'application y compris ceux de police judiciaire et intéressant la sécurité publique, le principe d'un droit de rectification, d'effacement ou de limitation s'exerçant de manière directe par la personne concernée auprès du responsable du traitement, la possibilité d'un exercice indirect de ses droits n'étant maintenue qu'en cas de restriction de ses droits.

- l'obligation pour le responsable du traitement, lorsqu'il fait droit à une demande de rectification, d'informer également l'autorité compétente dont les données proviennent,

- la possibilité pour le responsable du traitement d'exiger de la personne concernée le paiement de frais raisonnables ou de refuser de donner suite à une demande manifestement infondée ou abusive.

1.1.2.2 Dispositions générales relatives aux modalités de transmission des informations

Quel que soit le droit qu'il entend exercer au titre de la loi modifiée du 6 janvier 1978, l'intéressé doit fournir au responsable de traitement la justification de son identité.

Les règles nationales relatives à la preuve de l'identité de la personne concernée garantissent donc la protection des données personnelles en interdisant l'accès aux tiers non autorisés, conformément aux exigences européennes.

De même, l'article 95 du décret impose que toute référence à des codes, sigles ou abréviations figurant dans les documents délivrés par le responsable de traitement soit explicitée, si nécessaire sous la forme d'un lexique.
L'objectif de cette disposition, d'adresser une réponse à la personne concernée dans un langage clair, simple et aisément compréhensible, correspond pleinement aux dispositions de l'article 12 de la directive.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel attache une importance particulière à la protection des données à caractère personnel au regard de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 qui implique le respect de la vie privée.

Le Conseil constitutionnel a eu l'occasion de se prononcer plus précisément sur des dispositions limitant les demandes d'effacement anticipé concernant les personnes mises en cause, à propos du FNAEG. Il a jugé que les garanties prévues par le législateur étaient de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'était pas manifestement déséquilibrée. Parmi les garanties relevées, il a notamment souligné « *que l'inscription au fichier concerne, outre les personnes condamnées pour ces infractions, celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles les aient commises ; que, pour ces dernières, les empreintes prélevées dans le cadre d'une enquête ou d'une information judiciaires sont conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; qu'une procédure d'effacement est, dans ce cas, prévue par le législateur, lorsque la conservation des empreintes n'apparaît plus nécessaire compte tenu de la finalité du fichier ; que le refus du procureur de la République de procéder à cet effacement est susceptible de recours devant le juge des libertés et de la détention dont la décision peut être contestée devant le président de la chambre de l'instruction*»[122].

Une décision récente du Conseil constitutionnel portant sur le traitement des antécédents judiciaires (TAJ) illustre néanmoins le renforcement de la jurisprudence du Conseil constitutionnel en matière de protection de la vie privée. Le Conseil constitutionnel a en effet

[122] Décision n°2010-25 QPC du 16 septembre 2010, M. jean-Victor C., cons. 16

jugé qu'«*en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées port[ai]ent une atteinte disproportionnée au droit au respect de la vie privée*»[123].

1.3. CADRE CONVENTIONNEL

L'article 8 paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne prévoit que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

L'article 12 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, transposée en droit national par la loi n°2004-801 du 6 août 2004, impose également aux États membres de garantir notamment à toute personne concernée le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées, et selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, notamment en raison du caractère incomplet ou inexact des données.

De même, l'article 8 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 prévoit que toute personne doit pouvoir :

- connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier;
- obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;
- obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans la Convention;
- disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement.

La Cour européenne des droits de l'homme attache une importance particulière à la protection des données à caractère personnel, qui joue selon elle « *un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention* »[124].

[123] Décision n°2017-670 QPC du 27 octobre 2017, M. Mikhail P.

[124] CEDH, 18 septembre 2014, § 35

Il ressort notamment de la jurisprudence conventionnelle, particulièrement des décisions rendues contre la France[125], que le droit interne doit offrir une possibilité concrète de présenter une requête en effacement des données mémorisées[126], et que la Cour apprécie le respect de l'article 8 au regard des possibilités concrètes d'effacement des données dont bénéficie l'intéressé avant l'expiration de leur durée de conservation, en particulier lorsque la durée de conservation est longue[127].

La Cour a ainsi récemment affirmé que «*les personnes condamnées devraient […] se voir offrir une possibilité concrète de présenter une requête en effacement des données mémorisées [...], afin que la durée de conservation soit proportionnée à la nature des infractions et aux buts des restrictions*».

Elle en a conclu que dans la mesure où «*le régime actuel de conservation des profils ADN dans le FNAEG […] n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé*», il «*ne traduit donc pas un juste équilibre entre les intérêts publics et privés concurrents en jeu*»[128].

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

2.1.1. Mettre notre droit en conformité avec la création du droit à l'information de la personne concernée

Afin de mettre notre droit en conformité avec l'article 13 de la directive, il est créé un nouvel article 70-18 qui consacre dans notre ordre juridique l'obligation nouvelle pour le responsable de traitement de mettre à disposition de la personne concernée certaines informations en matière pénale.

Les informations devant être mises à disposition aux termes de ce nouvel article 70-18 correspondent stricto sensu à celles prévues par la directive.

L'article 18 du projet de loi assure les coordinations nécessaires avec l'actuel article 32 de la loi informatique et libertés.

Ainsi, les I et II abrogent les dérogations prévues par l'article 32 V pour les traitements ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté et par le VI pour les traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales. Ces précisions sont en effet désormais inutiles au regard des dispositions spécifiques créées aux articles 70-1 et suivants qui s'appliquent par dérogation aux autres dispositions de la loi informatique et libertés.

---

[125] La Cour a particulièrement examiné la conformité à l'article 8 des fichiers FIJAIS (CEDH, 17 décembre 2009, M.B. c. France, n° 22115/06), FAED (CEDH, 18 avril 2013, M.K. c. France, n° 19522/09, STIC (CEDH, 18 septembre 2014) et FNAEG (CEDH, 22 juin 2017).
[126] CEDH, 22 juin 2017, Aycaguer c.France, n° 8806/12, §38
[127] CEDH, 17 décembre 2009 précité, § 60
[128] CEDH, Aycaguer c. France précité, §44 et 45

Le I précise par ailleurs l'articulation de cet article 32 avec les dispositions nouvelles des articles 70-1 et suivants s'agissant des traitements intéressant la sécurité publique, qui peuvent relever du champ d'application de la directive.

2.1.2. Mettre notre droit en conformité sur le contenu du droit d'accès de la personne concernée

Afin de mettre notre droit en conformité avec l'article 14 de la directive qui diffère en partie sur le contenu du droit d'accès régi par l'article 39 de la loi, il est créé un nouvel article 70-19 qui reprend strictement les informations prévues par la directive, notamment relatives à la base juridique du traitement, à la durée de conservation des données, aux droits de la personne concernée de demander la rectification, l'effacement ou la limitation du traitement et d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés.

2.1.3. Mettre notre droit en conformité sur le droit de rectification ou d'effacement des données ou de limitation du traitement

Afin de mettre notre droit en conformité avec l'article 16 de la directive, l'article 70-20 I prévoit que la personne concernée a le droit d'obtenir du responsable du traitement :

- que soit rectifiées dans les meilleurs délais des données à caractère personnel qui sont inexactes ;

- que soient complétées des données à caractère personnel incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ;

- que soit effacées dans les meilleurs délais des données à caractère personnel, lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

Le II de l'article 70-20 impose au responsable du traitement de justifier qu'il a procédé aux rectifications, compléments et effacements exigés, lorsque l'intéressé en fait la demande, conformément à l'actuel article 40 de la loi informatique et libertés.

Le III de l'article 70-20 précise la possibilité nouvelle pour le responsable du traitement de limiter le traitement lorsqu'il ne peut être déterminé si les données sont ou non inexactes ou lorsque ces données doivent être conservées à des fins probatoires.

Le IV de l'article 70-20 transpose l'obligation pour le responsable du traitement d'informer la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus.

Enfin, les V et VI de l'article 70-18 imposent au responsable du traitement qui rectifie ou efface des données, ou limite leur traitement, de notifier ces diligences non seulement aux destinataires

de ces données qui devront opérer ces mêmes diligences sous leur responsabilité, mais aussi à l'autorité compétente dont les données proviennent.

2.1.4. METTRE NOTRE DROIT EN CONFORMITE AVEC LE PRINCIPE D'UN EXERCICE DIRECT DES DROITS

Afin de respecter le principe consacré par la directive d'un exercice direct des droits, le III de l'article 18 du projet de loi précise, s'agissant des traitements intéressant la sécurité publique, que l'exercice indirect des droits prévu par l'article 41 de la loi informatique et libertés s'applique sous réserve des dispositions du nouveau chapitre XIII.

De même, le IV de l'article 18 du projet de loi supprime l'application aux traitements de police judiciaire du régime dérogatoire d'exercice indirect prévu par l'article 42 de la loi informatique et libertés.

Ainsi, la personne concernée pourra directement exercer ses droits auprès du responsable du traitement, sans passer par l'intermédiaire de la Commission nationale de l'informatique et des libertés, pour tout traitement relevant du champ d'application de la directive, y compris ceux intéressant la sécurité publique ou ceux mis en œuvre par des administrations publiques et des personnes privées chargées d'une mission de service public ayant pour mission de prévenir, rechercher ou constater des infractions.

2.1.5. METTRE NOTRE DROIT EN CONFORMITE AVEC LE PRINCIPE DE GRATUITE DE L'ENSEMBLE DES INFORMATIONS TRANSMISES

Il est créé un nouvel article 70-23, qui prévoit, pour tous les droits de la personne concernée, le principe de gratuité des informations qui lui sont transmises, sauf exception liée à une demande manifestement infondée ou abusive.

Dans ce cas, l'article 70-23 permet également au responsable du traitement de refuser de donner suite à la demande.

2.2 NECESSITE DE LEGIFERER

L'objectif immédiat du projet de loi est de mettre notre droit national en conformité avec les exigences énoncées par la directive, plus particulièrement avec :

- la création en matière pénale d'un droit à l'information de la personne concernée par les données personnelles,

- la possibilité nouvelle pour le responsable du traitement de procéder dans certains cas à une limitation du traitement, plutôt qu'à un effacement des données,

- l'obligation nouvelle pour le responsable du traitement, lorsqu'il fait droit à une demande de rectification, d'informer l'autorité compétente dont les données proviennent,

- l'exercice par principe direct des droits par la personne concernée auprès du responsable du traitement, y compris pour les traitements intéressant la sécurité publique et la police judiciaire,

- la consécration du principe de gratuité de toutes les informations transmises en application de ces droits par le responsable du traitement à la personne concernée, sauf exception liée à une demande manifestement infondée ou abusive.

3. OPTIONS

La directive laisse à la libre appréciation des Etats membres la faculté de fixer certaines restrictions aux droits de la personne concernée, ainsi que la détermination des règles applicables à l'exercice des droits par la personne concernée pour certains types de données ou de traitements.

3.1. Transposer ou non les règles de la directive pour les données figurant dans une décision judiciaire, un casier ou un dossier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale

3.1.1. Option 1 (écartée) : Transposer les règles de la directive

L'article 18 de la directive laisse une option aux Etats membres s'agissant des droits de la personne concernée par des données à caractère personnel figurant dans une décision judiciaire, un casier ou dossier judiciaire faisant l'objet d'un traitement dans le cadre d'une enquête judiciaire et d'une procédure pénale.

Dans ces cas, la directive permet en effet de prévoir que les droits d'information, d'accès, de rectification, d'effacement ou de limitation du traitement prévus par les articles 13, 14 et 16 de la directive sont exercés conformément au droit national.

L'option d'imposer les exigences européennes pour ces données a été écartée.

3.1.2. Option 2 (retenue) : Maintenir le droit national

Cette option a été retenue.

Le Gouvernement a en effet souhaité maintenir la réglementation nationale propre à ces données traitées, compte tenu de l'équilibre nécessaire entre d'une part les intérêts et droits fondamentaux de la personne concernée, et d'autre part les nécessités de l'enquête, du secret de l'instruction et de la publicité des audiences.

Il est ainsi créé un nouvel article 70-24, aux termes duquel les dispositions relatives aux droits des personnes concernées transposées conformément aux exigences européennes ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas,

l'accès à ces données ne peut se faire que dans les conditions prévues par le code de procédure pénale.

3.2. Fixer ou non des restrictions aux droits de la personne concernée

3.1.1. Option 1 (écartée) : Ne prévoir aucune restriction aux droits des personnes concernée

L'article 13 paragraphe 3, l'article 15 paragraphe 1 et l'article 16 paragraphe 4 de la directive prévoient que les Etats membres peuvent adopter des mesures législatives restreignant l'ensemble des droits de la personne concernée, dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:
a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;
c) protéger la sécurité publique
d) protéger la sécurité nationale;
e) protéger les droits et libertés d'autrui.

L'option de ne pas user de cette faculté a été écartée.

Le gouvernement ne souhaite pas en effet que les droits légitimes de la personne concernée puissent s'exercer au détriment de la sécurité nationale ou publique, des droits et libertés d'autrui ou des nécessités de prévenir, rechercher, poursuivre les infractions pénales et d'exécuter les sanctions pénales.

3.1.2. Option 2 (écartée) : Déterminer des catégories de traitement susceptibles de donner lieu à des restrictions des droits à l'information et d'accès

L'article 13 paragraphe 4 et l'article 15 paragraphe 2 de la directive permettent aux Etats membres de fixer, par des mesures législatives, des catégories de traitement de données susceptibles de relever des finalités susvisées et ainsi de donner lieu à des restrictions des droits d'information et d'accès pour la personne concernée.

Cette option a été écartée.

En dehors des décisions et dossiers judiciaires qui font déjà l'objet d'une dérogation spéciale (cf supra), il est en effet apparu incohérent que la loi ne puisse déterminer des catégories de traitement qui pourraient nécessiter une dérogation générale, que pour les seuls droits d'information et d'accès, et non pour le droit de rectification, d'effacement ou de limitation.

Au vu de l'option ci-dessous retenue, l'utilisation d'une telle possibilité par la loi aurait conduit à autoriser moins de restrictions par la loi que par l'acte instaurant le traitement, notamment par l'acte réglementaire portant création du traitement.

L'acte instaurant le traitement aurait par ailleurs dû ajouter, pour chaque traitement, la possibilité de restriction pour le droit de rectification ou d'effacement, de sorte que cette option ne présentait qu'un intérêt pratique très limité.

Au surplus, il faut rappeler que si l'actuel article 42 de la loi informatique et libertés permet un accès indirect pour les fichiers de police judiciaire, il impose toutefois que ce droit d'accès indirect soit prévu par l'acte réglementaire en indiquant *« si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 et 27 »*.

3.1.3 Option 3 (retenue) : Prévoir des restrictions aux droits des personnes concernées dans l'acte instaurant le traitement

Compte tenu du maintien des formalités préalables à la création d'un traitement et de la logique actuelle de l'article 42 de la loi informatique et libertés, a été retenue l'option de laisser à l'acte instaurant le traitement , plutôt qu'à la loi, le soin de déterminer *in concreto* les traitements dans lesquels l'ensemble des droits, y compris celui de rectification ou d'effacement, pourraient être restreints.

Le nouvel article 70-21 permet ainsi à l'acte instaurant le traitement de déterminer si dans ce traitement, les droits des personnes concernées peuvent ou non faire l'objet de certaines restrictions.

Si le traitement est mis en œuvre pour le compte de l'Etat, l'arrêté ou le décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés détermine les restrictions applicables.

Dans les autres cas, seul un acte clair, précis et d'application prévisible pour les justiciables conformément au considérant 33 de la directive peut fixer des restrictions aux droits des personnes concernées.

A défaut d'un tel acte, aucune restriction ne peut être appliquée aux droits des personnes concernées.

Conformément aux exigences de la directive, l'acte instaurant le traitement peut prévoir des restrictions aux droits de la personne physique concernée dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne pour :
- éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
- éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;
- protéger la sécurité publique ;
- protéger la sécurité nationale ;
- protéger les droits et libertés d'autrui.

Lorsque l'acte instaurant le traitement prévoit la possibilité de telles restrictions aux droits, le responsable du traitement est en droit de :

1° Retarder ou limiter la fourniture ou ne pas fournir certaines informations à la personne concernée, à savoir celles mentionnées au II de l'article 70-18;

2° Limiter, entièrement ou partiellement, le droit d'accès de la personne concernée prévu par l'article 70-19 ;

3° Ne pas informer la personne de son refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de cette décision conformément au IV de l'article 70-20.

En cas de refus ou de limitation du droit d'accès, le responsable du traitement doit en informer la personne concernée dans les meilleurs délais, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent néanmoins ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs susmentionnés de prévention des infractions pénales, de protection de la sécurité ou des droits d'autrui. Le responsable du traitement doit alors consigner les motifs de fait ou de droit sur lesquels se fonde la décision, et mettre ces informations à la disposition de la Commission nationale de l'informatique et des libertés.

En cas de restriction des droits, le responsable du traitement doit informer la personne concernée de la possibilité d'introduire une réclamation en exerçant ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel.

L'esprit de la directive et particulièrement le considérant 44 ci-dessous partiellement reproduit commande une appréciation *in concreto* de la demande par le responsable du traitement : « *Le responsable du traitement devrait apprécier, en examinant chaque cas de façon concrète et individuelle, s'il y a lieu de limiter le droit d'accès partiellement ou complètement.* »

Le gouvernement ayant décidé d'utiliser l'option de fixer certaines restrictions aux droits de la personne concernée, il est nécessaire, au vu de l'article 17 de la directive, de permettre à cette dernière de les exercer également dans ces cas par l'intermédiaire d'une autorité de contrôle.

Ainsi le nouvel article 70-22 détermine les modalités d'exercice indirect de ses droits par la personne concernée par l'intermédiaire de la Commission nationale de l'informatique et des libertés en cas de restriction de ses droits.

Cet article maintient la législation nationale en vigueur en cas de saisine de la Commission, à savoir les deuxième et troisième alinéas de l'article 41.

Est enfin transposée dans cet article l'obligation pour la Commission d'informer la personne concernée de son droit de former un recours juridictionnel lorsqu'elle l'avise avoir procédé aux vérifications nécessaires.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

L'impact juridique de la disposition consiste dans l'insertion dans le nouveau chapitre XIII de la loi de 1978 de sept articles, les articles 70-18 à 70-24, et dans la modification des actuels articles 32, 41 et 42 de la loi de 1978.

DISPOSITIONS DU PROJET DE LOI	DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Article 18 PJL	Suppression, par coordination, des dérogations en matière pénale prévues par l'article 32 relatif au droit à l'information ; et précision de l'articulation avec le nouveau chapitre XIII pour les traitements intéressant la sécurité publique. La directive créant, dans ses articles 14 à 16, des droits d'accès et de rectification par principe directs en matière pénale, l'accès indirect prévu par l'article 42 de la LIL pour les traitements de police judiciaire est supprimé par l'article 21 du PJL, et celui prévu par l'article 41 de la LIL s'applique pour les traitements intéressant la sécurité publique sous réserve des dispositions du chapitre XIII.
Article 19 PJL	
Article 70-18	Article 13
Article 70-19	Article 14
Article 70-20	Article 16
Article 70-21	Transposition combinée des limitations ou restrictions aux droits d'information, d'accès ou de rectification prévues aux articles 13, 15 et 16 de la directive. Transposition également de l'obligation pour le responsable du traitement d'informer la personne concernée de la possibilité, prévue par l'article 17 de la directive, d'exercer ses droits par l'intermédiaire de la CNIL.
Article 70-22	Article 17
Article 70-23	Article 12
Article 70-24	Article 18

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES ET SUR LES ADMINISTRATIONS PUBLIQUES

Le principe d'un accès direct à tous les traitements va entraîner le transfert des demandes actuellement adressées à la Commission nationale de l'informatique et des libertés en sa qualité d'intermédiaire vers le responsable du traitement.

4.3. IMPACT SUR LES FINANCES PUBLIQUES

La gratuité des informations transmises imposée par la directive, en lieu et place de la possible délivrance d'une copie des données personnelles aux frais de la personne concernée dans le cadre de son droit d'accès, peut avoir un impact sur les finances publiques pour les traitements placés sous la responsabilité d'une administration publique.

4.4. IMPACTS SUR LES PARTICULIERS

Les droits de personnes faisant l'objet d'un traitement relevant de la directive seront renforcés par les nouvelles dispositions.

5. CONSULTATION ET MODALITÉS D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

La réforme s'appliquera le 25 mai 2018, conformément à l'article 24 du projet de loi.

Ces dispositions seront applicables sur l'ensemble du territoire, hors les collectivités d'outre-mer soumises au principe de spécialité, pour lesquelles l'extension se fera par ordonnance

ARTICLE 19 SECTION 4

TRANSFERTS INTERNATIONAUX

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1 Droit actuel concernant les transferts internationaux de données

La loi n°78-17 du 6 janvier 1978 a été modifiée par la loi n°2004-801 du 6 août 2004 pour mettre la législation française en conformité *avec la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces donnée*s qui ne s'applique pas en matière pénale[129].

A cette occasion, le Parlement a notamment introduit les deux articles 68 et 69 qui disposent :

« Article 68. **-** *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.*
Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. »

Article 69. **-** *Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :*
1° A la sauvegarde de la vie de cette personne ;
2° A la sauvegarde de l'intérêt public ;
3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

[129] En effet, l'article 3, paragraphe 2 (champ d'application de cette directive) dispose : « La présente directive ne s'applique pas au traitement de données à caractère personnel: - mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,… »
Il en résulte que l'article 25 de cette directive qui prohibe les transferts de données vers des Etats tiers n'assurant pas un niveau de protection adéquat ne s'applique pas aux transferts de données en matière pénale, en particulier les données en matière pénale, policières ou judiciaires.

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.
Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'Etat pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel qu'elle prend au titre de l'alinéa précédent. »

Par ailleurs, l'Union européenne a adopté un autre instruments relatif aux transferts de données, qui s'applique en matière pénale en l'espèce *la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale* dont les restrictions ne s'appliquent qu'aux données qui proviennent d'autres Etats membres.

Outre la législation européenne et la loi française, les transferts internationaux sont régis par le décret n°2005-1309 du 20 octobre 2005 (modifié par le décret n°2007-451 du 25 mars 2007[130]) pris pour l'application de la loi susvisée

Les dispositions de ce décret relatives au transfert de données, mentionnées aux articles 91[131] et 108[132] précisent les obligations qui incombent aux responsables de traitements. Ces dispositions font référence à la liste des Etats établie par la Commission et considérée comme assurant un

[130] JO n°74 du 18 mars 2007 page 5782
[131] L'article 91 du décret dispose : « *Les informations figurant au 7° du I de l'article 32 de la loi du 6 janvier 1978 susvisée que le responsable du traitement communique, dans les conditions prévues à l'article 90, à la personne auprès de laquelle des données à caractère personnel sont recueillies, sont les suivantes :*
1° Le ou les pays d'établissement du destinataire des données dans les cas où ce ou ces pays sont déterminés lors de la collecte des données ;
2° La nature des données transférées ;
3° La finalité du transfert envisagé ;
4° La ou les catégories de destinataires des données ;
5° Le niveau de protection offert par le ou les pays tiers :
a) Si le ou les pays tiers figurent dans la liste prévue à l'article 108, il est fait mention de la décision de la Commission européenne autorisant ce transfert ;
b) Si le ou les pays tiers ne satisfont pas aux conditions prévues à l'article 68 de la même loi, il est fait mention de l'exception prévue à l'article 69 de cette loi qui permet ce transfert ou de la décision de la Commission nationale de l'informatique et des libertés autorisant ce transfert.
[132] L'article 108 du décret dispose : « *La commission met à la disposition du public la liste des décisions de la Commission européenne concernant le niveau de protection offert par les États n'appartenant pas à la Communauté européenne au regard de la vie privée, des libertés et droits fondamentaux et à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel. Elle actualise cette liste au fur et à mesure de la publication des décisions de la Commission européenne au Journal officiel de l'Union européenne.*
Elle met également à la disposition du public les clauses contractuelles types approuvées par la Commission européenne.

niveau adéquat de protection des données au regard de la directive 95/46/CE qui ne s'applique pas en matière pénale.

Le fait d'assurer un niveau de protection adéquat au regard de cette directive 95/46/CE ne semble pas permettre de conclure que la protection est adéquate pour les traitements et fichiers élaborés en matière pénale (et réciproquement). D'une part les règles de protection en matière commerciale et civile ne sont pas identiques aux règles applicables en matière pénale (les principes d'information et de correction des données, le traitement des données sensibles telles que les empreintes génétiques, la conservation en l'absence d'accord de la personne concernée, etc. sont fondamentalement différents. D'autre part, certains Etats peuvent ne pas garantir les mêmes droits dans le domaine commercial alors qu'ils peuvent les garantir pour les fichiers en matière pénale.

Le dernier alinéa de l'article 91 du décret dispose : « *Lorsque le transfert est envisagé postérieurement à la collecte des données à caractère personnel, celui-ci ne peut intervenir que dans un délai de quinze jours suivant la réception par l'intéressé des informations ci-dessus ou, le cas échéant, au terme de la procédure visée à l'article 94.* »

Par ailleurs, le guide relatif aux « transferts de données à caractère personnel vers des pays tiers à l'Union européenne » édité sur le site de la CNIL ne semble pas adapté aux transferts de données en matière pénale. Il souligne notamment que « *Les personnes dont les données doivent être transférées doivent être informées de l'existence de ce transfert ; (Article 91 du décret 2007)* ».

Enfin, dans son avis n° 372616 en date du 26 octobre 2006, le Conseil d'Etat a considéré que le transfert de données à caractère personnel dont le traitement a pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne relève pas de la catégorie des transferts nécessaires à la sauvegarde de l'intérêt public au sens du 2° de l'article 69 de la loi informatique et libertés[133].

---

[133] Lors de l'examen du projet de loi de ratification de l'accord d'entraide judiciaire en matière pénale entre le Gouvernement de la République française et le Gouvernement de la République populaire de Chine, signé à Paris le 18 avril 2005, le Conseil d'État a examiné cet accord et après de longs débats a émis un avis favorable en adressant au Gouvernement une note en formulant des observations[133]. Cette note en date du 26 octobre 2006 comprend notamment une interprétation des articles 26, 68 et 69 de la loi informatique et libertés mentionnant (cf. page 3 de la note en annexe I) précisant :« *la ratification, après autorisation parlementaire, de l'accord dont les articles XVII et XVIII autorisent l'échange d'informations figurant dans les casiers judiciaires et d'avis de condamnation ne saurait avoir pour effet de dispenser les autorités françaises, chargées de transférer des données contenues dans des traitements automatisés de données à caractère personnel gérés par les autorités judiciaires vers un État n'appartenant pas à la Communauté européenne, des obligations de vérification qui leur incombent en application des articles 26, 68 et 69 précités à l'occasion de chaque demande de transfert.*
Cette vérification devra tenir compte, à la date du transfert des données, non seulement du niveau spécifique de protection garanti par le traitement appliqué aux données objet du transfert, mais aussi de l'ensemble des circonstances qui commandent l'application effective des règles de protection définies pour ce transfert.
Il est souligné que, le transfert de données à caractère personnel dont le traitement a pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté relève non pas de la catégorie des transferts nécessaires à la sauvegarde de l'intérêt public au sens du 2° de l'article 69 précité, mais de celle des transferts de données dont le traitement est autorisé par décret en Conseil d'État dans les conditions de fond et de procédure prévues à l'avant-dernier alinéa de l'article 69 ».

Or seul un très petit nombre d'Etats (environ une douzaine d'Etats[134]) n'appartenant pas à l'Union européenne ont été classés par l'Union européenne ou par la Commission Nationale de l'Informatique et des libertés comme ayant un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont des données personnelles. La plupart des Etats tiers (environ deux cent cinquante Etats) ne relèvent donc pas de cette catégorie.

1.2 Régime instauré par la directive 2016/680 du 27 avril 2016

La directive introduit un mécanisme permettant le transfert de données à caractère personnel d'une part à des autorités compétentes se trouvant dans d'autres Etats, d'autre part à des destinataires se trouvant dans d'autres Etats.

Le premier cas correspond à la traditionnelle coopération entre services des autorités judiciaires ou services en charge des enquêtes en charge de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière ou en charge de l'exécution des sanctions pénales. Le second cas permet dans des situations particulières d'adresser directement des informations à caractère personnel à des destinataires situés dans d'autres Etats, aux mêmes fins (enquêtes et exécution des sanctions pénales). Ce second cas permet aux autorités compétentes d'adresser directement des demandes comprenant des informations à caractère personnelle à des services fournissant par exemple des services de communications électroniques délocalisés mais utilisés dans un Etat pour commettre des infractions (messages échangés entre des utilisateurs situés en France pour commettre des actes de terrorisme, pour transmettre des images ou vidéos pédopornographiques en utilisant des messageries électroniques situés à l'étranger).

Les transferts de données à caractère personnel sont traditionnellement effectués dans le cadre de commission rogatoire internationale ou des échanges entre service de police judiciaire permettant de solliciter une autorité judiciaire ou un services équivalent en charge des enquêtes en charge de la prévention et de la détection des infractions pénales dans un autre Etat. Il est bien évidemment nécessaire de communiquer certaines informations à caractère personnel pour que les autorités judiciaires étrangères ou les services de police judiciaire puissent enquêter. Ces demandes dites actives impliquent donc que des transferts de données personnelles soient effectués.

Par ailleurs, les autorités judiciaires comme les services de police judiciaire peuvent être sollicités par leurs homologues des autres Etats, généralement dans le cadre de conventions d'entraide judiciaire en matière pénale, de convention d'extradition ou de transfèrement, ou d'accords de sécurité intérieur pour coopérer en matière d'enquête ou d'exécution de sanctions pénales. Ces demandes dites passives (n'émanant pas de l'initiative d'autorités compétentes françaises) impliquent également le transfert de données à caractère personnel.

La directive prévoit que les autorités compétentes peuvent échanger de telles données dans quatre cas :

[134] C'est notamment le cas de la Suisse, du Canada, de l'Argentine, des territoires de Jersey et Guernesey, de l'Isle de Man, de la Norvège, de l'Islande et d'Israël, et de quelques autres Etats.

1°) Lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat (régime de l'article 36 de la directive) ;

2°) Lorsque des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant (régime de l'article 37 1° a) ; Cette situation sera rencontrée lorsque la convention d'entraide, d'extradition ou de transfèrement, ou l'accord de sécurité intérieur prévoit des dispositions juridiques contraignantes en matière de protection des données à caractère personnelle. Quelques conventions récentes prévoient de telles stipulations. Mais les conventions anciennes (la convention d'entraide judiciaire en matière pénale du Conseil de l'Europe par exemple) ne prévoient pas de protection.

3°) Lorsque le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel (régime de l'article 37 1° b) ;

4°) En l'absence de décision d'adéquation ou de garanties appropriées lorsque le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, à la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit de l'État membre transférant les données à caractère personnel le prévoit, pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers, et dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice pour une enquête en matière pénale ou pour l'exécution d'une sanction pénale.

Par ailleurs, la directive prévoit que « les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant le 6 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation » (article 61 de la directive). Les conventions d'entraide, d'extradition ou de transfèrement, les accords de sécurité intérieure, adoptés antérieurement à l'adoption de la directive même s'ils ne comportent pas de stipulations spécifiques à la protection des données à caractère personnel étaient conforme au droit de l'Union européenne (à défaut de quoi ils n'auraient pas pu être signés et ratifiés, notamment en raison de la primauté du droit de l'union européenne). Ils restent donc en vigueur jusqu'à ce qu'ils soient remplacés ou révoqués.

La loi de transposition ne devrait pas avoir d'impact sur les transferts de données à caractère personnel effectués par les autorités judiciaires comme par les services de police judiciaire qui respectaient déjà d'une part les conventions applicables et d'autre part des principes constitutionnels plus élevés que le droit européen, les conventions internationales et la loi. Ainsi chaque fois que l'envoi d'une demande de coopération (commission rogatoire ou demande de renseignements adressée par un service de police judiciaire), ou l'envoi d'une réponse à une demande de coopération était susceptible de mettre ne cause des principes fondamentaux (application de la peine de mort, application de sanction(s) incompatible(s) avec le respect de la personne humaine, des garanties étaient exigées préalablement à l'envoi de la demande ou de la réponse. En outre, si quelques conventions anciennes ne comprennent pas de mention explicite du principe de spécialité (impossibilité d'utiliser les informations transmises dans un autre cadre que l'affaire pour laquelle les données personnelles ont été sollicitées) ou de confidentialité

(impossibilité de transmettre les données à d'autres autorités que les autorités compétentes qui ont sollicité les données), toutes les conventions signées et ratifiées depuis une trentaine d'années comprennent ces deux principes.

Outre ces transferts entre autorités compétentes, la directive autorise des transferts qui n'étaient pas envisagés jusqu'à présent, à savoir des transferts d'une autorité compétente à des destinataires établis dans d'autres Etats. Il s'avère que de nombreuses infractions pénales sont commises par des criminels et des délinquants qui utilisent des services de transmission situé à l'extérieur des Etats où sont commises les infractions. C'est le cas notamment dans le domaine du terrorisme, des infractions en matière de diffusion d'images ou de vidéos pornographiques, en matière d'incitation à la haine ou à la xénophobie, de racisme, etc. S'il reste dans certains cas des frontières pour les personnes et les biens, les données échangées par des systèmes électroniques ne connaissent pas de frontières. Les enquêtes conduisent ainsi les autorités judiciaires ou les services de police à devoir identifier des criminels et des délinquants qui se cachent derrière des pseudonymes et utilisent des systèmes de messagerie électronique souvent situés dans d'autres Etats. Il est donc nécessaire de transmettre des données personnelles (adresse IP, pseudonymes, identifications des moyens de communication notamment adresse de messagerie) aux fournisseurs d'accès situés dans d'autres Etats. La directive permet de tels transferts dans un cadre très précis (article 39 de la directive) qui sera introduit à l'article 70-24 de la loi informatique et libertés. Il convient d'observer que la réponse effectuée par le destinataire situé à l'étranger et qui n'est pas une autorité compétente ne relève pas des dispositions de la directive mais d'autres dispositions : au sein des Etats membres de l'Union européenne, cette réponse relève du règlement, au sein des Etats non membres de l'Union européenne, la réponse relève des lois nationales de ces Etats.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

Il est nécessaire de transposer de façon exacte les dispositions des articles 35 à 39 de la directive, ce qui suppose d'insérer dans la loi de 1978, dans le nouveau chapitre XIII relatif aux traitements relevant de la directive, au sein d'une section consacrée aux transferts de données hors de France, des dispositions reprenant les articles précités de la directive, et dérogeant, pour ces traitements, aux actuels articles 68 à 70 de la loi

3. OPTIONS

3.1. OPTION 1 (ecartée) : Maintien du système actuel

Le système actuel ne semble pas compatible avec la directive qui prévoit un régime différent confiant la responsabilité des transferts au responsable de traitement.

Par ailleurs en matière pénale, le principe constitutionnel de séparation des pouvoirs rappelé par la directive[135], le secret de l'enquête et de l'instruction semblent difficilement compatibles avec

[135] L'article 45, paragraphe 2 de la directive mentionne : « Chaque État membre prévoit que chaque autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle. Les États membres peuvent prévoir que leur autorité de contrôle n'est pas

les formalités prévues par les deux derniers alinéas de l'article 69 de la loi informatique et libertés (pour les traitements mentionnés au I ou au II de l'article 26 de la loi informatique et libertés obligation d'un décret en Conseil d'Etat pris après avis motivé et publié de la CNIL et obligation de porter à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel).

La solution consistant à maintenir le système actuel n'a donc pas été retenue.

3.2. OPTION 2 (retenue) : Définition d'un nouveau régime strictement conforme aux articles 35 à 39 de la directive

Cette solution, qui présente l'avantage de simplifier le mécanisme d'entraide judiciaire tout en maintenant des garanties appropriées, a été retenue.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

L'impact juridique de cette disposition consiste dans l'insertion dans le nouveau chapitre XIII de la loi de 1978 de trois articles, les articles 70-25 à 70-27

5. CONSULTATION ET MODALITÉS D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

La réforme s'appliquera le 25 mai 2018, conformément à l'article 24 du projet de loi.

Ces dispositions seront applicables sur l'ensemble du territoire, hors les collectivités d'outre-mer soumises au principe de spécialité, pour lesquelles l'extension se fera par ordonnance.

---

compétente pour contrôler les opérations de traitement effectuées par d'autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle »

TITRE IV

HABILITATION A AMELIORER L'INTELLIGIBILITE DE LA LEGISLATION APPLICABLE A LA PROTECTION DES DONNEES

ARTICLE 20

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés constitue le texte fondateur et unique en matière de protection des données à caractère personnel.

La mise en conformité de cette loi avec le « paquet européen » des données à caractère personnel adopté le 27 avril 2016 conduit à intégrer dans ce texte des dispositions qui relèvent de champs d'application différents (règlement (UE) 2016/679 d'une part, directive (UE) 2016/680 d'autre part), tout en maintenant des dispositions qui concernent également des traitements ne relevant pas du droit de l'Union européenne (fichiers relatifs à la défense nationale par exemple). L'article 21 du présent projet de loi contient déjà certaines mesures de coordination rendues directement nécessaires par les modifications apportées à la loi n° 78-17.

Le présent projet de loi permet, à travers les titres I à III, au Parlement de débattre sur les mesures les plus importantes relatives à la transposition de la directive et aux marges de manœuvres permise par le règlement afin de laisser la représentation nationale se prononcer sur les grandes orientations en matière de protection des données.

Une fois ces choix opérés et la loi promulguée, un travail plus technique de mise en cohérence et de coordination de la loi n° 78-17 sera nécessaire, afin notamment de mieux articuler les dispositions selon le champ d'application dont elles relèvent). Il est proposé d'effectuer ce travail par ordonnance.

A cet égard, il sera rappelé que la loi n° 78-17 a fait l'objet de nombreuses modifications par ordonnance[136].

Les modifications apportées par ordonnances ont ainsi par exemple permis la mise en conformité du droit national aux dispositions de la directive 2009/136/CE concernant le service universel et

[136] Ordonnance n° 96-267 du 28 mars 1996 relative à l'entrée en vigueur du nouveau code pénal dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte ainsi qu'à l'extension et à la modification de certaines dispositions législatives rendues nécessaires par cette entrée en vigueur ; ordonnance n° 2000-916 du 19 septembre 2000 portant adaptation de la valeur en euros de certains montants exprimés en francs dans les textes législatifs ; ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques ; ordonnance n° 2015-948 du 31 juillet 2015 relative à l'égal accès des femmes et des hommes au sein des autorités administratives indépendantes et des autorités publiques indépendantes ; ordonnance n° 2016-462 du 14 avril 2016 portant création de l'Agence nationale de santé publique.

les droits des utilisateurs au regard des réseaux et services de communications électronique et de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

1.2. CADRE CONSTITUTIONNEL

Le Conseil Constitutionnel considère que le législateur peut autoriser le Gouvernement à tirer les conséquences, par ordonnances, de la loi qu'il a adoptée et assurer ainsi la coordination des dispositions législatives en vigueur avec celles de cette loi[137].

Il juge également de manière constante que « *si l'article 38 de la Constitution fait obligation au Gouvernement d'indiquer avec précision au Parlement, afin de justifier la demande qu'il présente, la finalité des mesures qu'il se propose de prendre par voie d'ordonnance ainsi que leur domaine d'intervention, il n'impose pas au Gouvernement de faire connaître au Parlement la teneur des ordonnances qu'il prendra en vertu de cette habilitation ;* »[138].

Le Conseil constitutionnel a estimé qu'est assez précise une demande autorisant le Gouvernement à transposer des directives, y compris si elles sont susceptibles d'être adoptées au cours du délai d'habilitation[139].

Enfin, il sera rappelé que l'objectif d'intelligibilité et d'accessibilité de la loi que l'article d'habilitation souhaite atteindre par une réécriture par ordonnance de la loi n° 78-17 constitue un objectif de valeur constitutionnelle que le Conseil constitutionnel rattache aux articles 4, 5, 6 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789[140], à l'instar de la technique de codification. Le Conseil constitutionnel considère en effet que : « *la codification répond à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, qui découle des articles 4, 5, 6 et 16 de la Déclaration de 1789 ; qu'en effet l'égalité devant la loi énoncée par l'article 6 de la Déclaration et « la garantie des droits » requise par son article 16 pourraient ne pas être effectives si les citoyens ne disposaient pas d'une connaissance suffisante des normes qui leur sont applicables ; qu'une telle connaissance est en outre nécessaire à l'exercice des droits et libertés garantis tant par l'article 4 de la Déclaration, en vertu duquel cet exercice n'a de bornes que celles déterminées par la loi, que par son article 5, aux termes duquel « tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint à faire ce qu'elle n'ordonne pas* »[141].

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

L'habilitation que le Gouvernement sollicite par le présent projet de loi répond à un objectif de qualité de la législation et de meilleure lisibilité et intelligibilité de la loi n° 78-17 grâce à une

[137] Décision du 16 juillet 2009, n° 2009-584 DC, cons. 20 à 23.
[138] Voir par exemple, décision du 17 mai 2013, n°2013-669 DC, cons. 79.
[139] Décision du 23 juin 2003, n°2003-473 DC, cons. 8.
[140] Décision n° 2004-500 DC du 29 juillet 2004, cons. 13 ; ° 2005-514 DC, 28 avril 2005, cons. 14
[141] Décision n° 2007-561 DC du 17 janvier 2008, cons. 6.

nouvelle architecture qui sera divisée en titres, dispositions communes et selon la finalité des traitements (règlement, directive, hors champ du droit de l'Union européenne).

Il s'agit également d'assurer la conformité du droit national avec le règlement et la directive, en permettant d'une part, d'abroger les dispositions redondantes dans le règlement et la loi, sauf si la mesure est commandée pour la clarté, d'autre part, de modifier les dispositions de la loi n° 78-17 ou d'autres textes qui ne seraient plus en conformité avec le nouveau droit de la protection des données.

2.2 NECESSITE DE LEGIFERER

Le « paquet européen protection des données » constitue une modification importante du droit de la protection des données à caractère personnel.

Dans le respect des dispositions votées aux titres I à III du projet de loi, et sans préjudice des mesures de coordination déjà prévues par l'article 21 du projet de loi, la loi n°78-17 nécessite une réécriture afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification, à la cohérence et à l'intelligibilité de cette loi consécutive à sa mise en conformité au règlement (UE) 2016/679 et à la transposition de la directive (UE) 2016/280.

Il conviendra aussi, sur le fondement des dispositions votées par le Parlement et des dispositions du règlement directement applicable de mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel. Il s'agit également d'apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, de remédier aux éventuelles erreurs et omissions résultant de la présente loi, et d'abroger les dispositions devenues sans objet.

Enfin, l'habilitation est prévue pour l'adaptation et les extensions éventuelles à l'outre-mer des dispositions résultant de ces modifications.

3. OPTIONS

3.1. Habilitation à prendre par ordonnance des mesures législatives de réécriture de la loi n°78-17

3.1.1. Option 1 (écartée) Maintenir la loi n° 78-17 dans sa rédaction qui résultera de l'adoption du présent projet de loi

Les titres I à III du présent projet de loi assurent un niveau de transposition et de mise en conformité minimum au regard du « paquet européen ».

Certaines dispositions, en particulier celles relatives aux définitions, aux droits des personnes concernées et des exceptions ne correspondront plus à l'état du droit en mai 2018, date d'application du « paquet européen ».

Certes, le principe de primauté du droit de l'Union européenne[142] permettrait au juge national et à l'autorité de contrôle d'écarter, pour les traitements relevant du champ du règlement et de la directive, les dispositions de la loi nationale contraires aux textes européens.

Cette solution n'apparaît toutefois pas satisfaisante au regard de la prévisibilité et de l'intelligibilité de la norme.

3.1.2. Option 2 (écartée) Mettre en conformité l'ensemble de la législation nationale par ordonnance

Cette option qui avait été envisagée par amendement lors de la première lecture du projet de loi pour une République numérique a été écartée.

Le Gouvernement a en effet fait le choix de soumettre à la représentation nationale les choix permis par le droit européen s'agissant d'un domaine aussi important que la protection des données à caractère à caractère personnel

3.1.3. Option 3 (retenue) : Habilitation à réécrire la loi n° 78-17 dans le respect des dispositions des titres I à III du texte proposé

Afin d'améliorer l'intelligibilité de la loi, la réécriture de l'ensemble de la loi n° 78-17 en cohérence avec le règlement et la directive (UE) 2016/680 semble nécessaire, sans préjudice des mesures de coordination déjà prévues par le projet de loi.

A ce titre, le Conseil constitutionnel a jugé que répondait à cet objectif, l'élaboration d'un nouveau plan d'un code afin de le rendre plus accessible à ses utilisateurs, en regroupant dans des blocs homogènes des dispositions jusqu'alors éparses[143].

Différents textes spécifiques doivent également être mis en cohérence, une grande partie des traitements de données à caractère personnel étant en effet prévus dans des textes sectoriels renvoyant à des dispositions de la loi n° 78-17 amenées à être modifiées ou abrogées par le règlement à compter du 25 mai 2018.

Enfin, afin d'assurer l'effectivité du droit à la protection des données à caractère personnel sur l'ensemble du territoire, il apparait nécessaire de procéder à l'adaptation et aux extensions utiles dans les collectivités d'outre-mer.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1 IMPACTS JURIDIQUES

L'article 20 du projet de loi autorise le Gouvernement, dans le respect des dispositions prévues aux titres I à III du projet de loi, à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires :

[142] CJCE, arrêt Costa contre Enel, 15 juillet 1964.
[143] Décision n° 2007-561 DC du 17 janvier 2008, cons. 8.

- pour réécrire l'ensemble de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification, à la cohérence et à l'intelligibilité de cette loi consécutive à sa mise en conformité au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et à la transposition de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 telle que résultant de la présente loi ;
- pour mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel, apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi, et abroger les dispositions devenues sans objet ;
- À l'adaptation et aux extensions à l'outre-mer des dispositions prévues aux 1° et 2°, ainsi qu'à l'application en Nouvelle-Calédonie, à Wallis-et-Futuna en Polynésie française, à Saint-Barthélemy, à Saint-Pierre-et-Miquelon et dans les Terres australes et antarctique françaises.

4.2 IMPACTS SUR LES PARTICULIERS

La réécriture de la loi n° 78-17 doit permettre une meilleure accessibilité et donc une meilleure compréhension des droits des personnes concernées et des obligations incombant aux responsables de traitement.

4.3 IMPACTS SUR LES ENTREPRISES

A l'instar de l'impact attendu pour les particuliers, cette disposition doit permettre une meilleure accessibilité et donc une meilleure compréhension des obligations incombant aux responsables de traitement et aux sous-traitants.

5. CONSULTATION ET MODALITES D'APPLICATION

5.1. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

Elle le sera également sur le projet d'ordonnance prévue par l'article 20 du projet de loi.

5.2. MODALITES D'APPLICATION

Les textes réglementaires suivants devront être pris sur le fondement de la loi :

Articles du PJL renvoyant à des mesures réglementaires	**Nature du texte réglementaire**	**Objet du texte réglementaire**
Article 20	Ordonnance	Habilitation à améliorer l'intelligibilité de la législation applicable à la protection des données

TITRE V

DISPOSITIONS DIVERSES ET FINALES[144]

ARTICLE 22

MISE A DISPOSITION DE LA LISTE DES TRAITEMENTS AYANT FAIT L'OBJET DE FORMALITES PREALABLES

1. ETAT DE LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

Depuis la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés tient à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26 (traitements dits de « souveraineté » ne faisant pas l'objet d'une publication).

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a fait basculer ce registre des formalités préalables dans l'*open data* en prévoyant une mise à disposition du public, dans un format ouvert et aisément réutilisable[145].

Lorsqu'un responsable de traitement dispose d'un correspondant à la protection des données, ce droit s'exerce directement auprès de ce dernier, qui doit tenir la liste des traitements mis en œuvre (article 22-III de la loi n° 78-17).

Cette disposition législative permet une mise à disposition du public, dans un format ouvert et aisément réutilisable la liste des traitements ayant fait l'objet d'une formalité auprès de la Commission nationale de l'informatique et des libertés. Ce droit de communication ne correspond pas au droit d'accès aux documents administratifs prévu par le code des relations entre le public et l'administration dès lors que la liste en question constitue, par nature, un document inachevé, puisqu'il évolue avec les nouvelles formalités préalables qui interviennent auprès de la commission et qu'il contient des données à caractère personnel (identité du responsable de traitement, adresse,), deux caractéristiques qui font obstacle au droit à l'accès des documents administratifs[146].

---

[144] L'article 21 du présent projet de loi procède à des mesures de coordination du fait notamment de la disparation de certaines formalités préalables. Les impacts de cette disposition sont uniquement de nature juridique.

[145] Le Conseil constitutionnel n'a pas eu l'occasion de se prononcer sur la nouvelle rédaction de l'article 31 de la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction issue de la loi pour une République numérique.

[146] Article L. 311-1 du code des relations entre le public et l'administration : « *Le droit à communication ne s'applique qu'à des documents achevés.* » ; article L. 311-6 de ce code : « *Ne sont communicables qu'à l'intéressé les documents administratifs : / 1° Dont la communication porterait atteinte à la protection de la vie privée, (…)* ».

Enfin, au titre du II de l'article 31 de la loi n° 78-17, la Commission nationale de l'informatique et des libertés tient à la disposition du public l'intégralité de ses avis, décisions ou recommandations.

1.2 CADRE CONVENTIONNEL

Le règlement (UE) 2016/679 ne prévoit pas d'obligation de mise à disposition d'un tel registre puisque la logique de responsabilisation du règlement (UE) 2016/679 permet la suppression de la grande majorité des formalités préalables et que le droit d'accès apporte une réponse aux personnes concernées désireuses de connaître ces informations (articles 13 et 14).

Pour autant, le règlement ne s'oppose pas non plus à une mesure d'information du public et des personnes concernées, puisque le droit à l'information est une composante majeure de la protection des données à caractère personnel (article 15).

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

Cette disposition vise à permettre la réutilisation des informations concernant les traitements ayant fait l'objet de formalités préalables actuellement mise à disposition du public par la Commission nationale de l'informatique et des libertés, lesquelles ne pourraient pas être réutilisées dans le cadre du droit commun d'accès aux documents administratifs compte tenu des données contenues dans le registre.

Cette disposition assure également une pérennité à ce document, puisque de nombreux traitements sont actuellement en cours, contribuant ainsi à l'information des personnes concernées.

2.2 NECESSITE DE LEGIFERER

L'entrée en application du règlement (UE) 2016/679 et sa logique de responsabilisation, ainsi que la suppression de la majorité des formalités préalables devrait conduire à la disparition du registre des traitements actuellement mis à disposition par la Commission nationale de l'informatique et des libertés au titre de l'article 31 de la loi n° 78-17.

De nombreux traitements en cours se poursuivront après le 25 mai 2018, date d'entrée en application du règlement, il serait préjudiciable pour le droit à l'information des personnes concernées de ne plus avoir connaissance de l'ensemble des traitements mis en œuvre.

Il apparaît dès lors nécessaire de prévoir un nouveau registre des autorisations existantes, en plus des publications officielles.

Ce registre constitue un outil pertinent pour les actuels correspondants à la protection des données, il le sera également pour les futurs délégués à la protection des données. Cette disposition apparaît cohérente avec l'article 10 du projet de loi qui prévoit par ailleurs que ce

délégué pourra communiquer la liste des traitements effectués par le responsable de traitement qui l'a désigné à toute personne qui lui en fait la demande.

3. OPTIONS

Option 1 (écartée) : Absence de mesure législative

L'obligation de tenue à disposition du public du registre prévu à l'article 31 aurait vocation à disparaître dès lors que le règlement ne comporte pas une telle obligation pour les autorités de contrôle. Cette liste des traitements déclarés ou autorisés aurait ainsi probablement disparue faute de maintenance.

Cette option a été écartée.

Option 2 (écartée) : Maintien du registre prévu à l'article 31 pour une durée d'un an

Il aurait pu être envisagé de maintenir ce registre dans un format ouvert et aisément réutilisable pendant une durée d'un an, afin de faire la transition entre le droit existant sous l'empire de la directive 95/46/CE et le règlement (UE) 2016/679. Cette durée semble insuffisante compte tenu du nombre de traitements recensés qui continueront à être mis en œuvre au-delà du 25 mai 2018 et même du 25 mai 2019. L'effet utile de ce registre en serait considérablement réduit.

Option 3 (retenue) : Maintien du registre prévu à l'article 31 pour une durée de dix ans

Il est proposé, que pour les traitements ayant fait l'objet de formalités antérieurement à l'entrée en vigueur de la future loi, l'obligation pour la Commission nationale de l'informatique et libertés, prévue à l'article 31 de la loi n°78-17, de mettre à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements arrêtée à cette date, pour une durée de dix ans.

Le droit à l'information des personnes concernées, mais également des usagers des services publics à connaître des traitements mis en œuvre par les administrations, sera prolongé couvrant ainsi des traitements existants.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGEE

4.1. IMPACTS JURIDIQUES

Cette disposition vise à maintenir en l'état l'obligation faite à la Commission nationale de l'informatique et des libertés de mettre à disposition un registre en *open data* la liste des traitements ayant fait l'objet de formalités préalables, prévue par la loi pour une République numérique, pour une durée de 10 ans.

4.2 IMPACTS SUR LES PARTICULIERS

La présente disposition aura un impact sur les particuliers puisqu'ils pourront continuer à consulter la liste des traitements, mis en œuvre avant le 25 mai 2018, ayant fait l'objet de formalités préalables publiques.

Il s'agit d'une mesure qui contribue à l'exercice effectif du droit à l'information, tant au titre de l'accès à l'information publique pour les traitements mis en œuvre par des administrations, qu'à l'égard des personnes concernées.

4.3 IMPACT SUR LES ENTREPRISES

Les entreprises auront la possibilité de réutiliser les informations contenues dans ce registre, dans le respect de la loi n°78-17.

5. CONSULTATION

La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

ARTICLE 23

MODIFICATION DE L'ARTICLE 230-8 DU CODE DE PROCEDURE PENALE

L'article 23 du présent projet de loi réécrit le premier alinéa de l'article 230-8 afin de tirer les conséquences de la décision 2017-670 QPC du 27 octobre 2017 par laquelle le Conseil constitutionnel a censuré cet alinéa.

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1. ETAT DES LIEUX

L'article 230-8 du CPP est issu de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI », qui a inséré au sein de ce code un chapitre dédié aux « fichiers de police judiciaire », dont la première section traite des « fichiers d'antécédents » (articles 230-6 à 230-9).

L'article 230-6 du CPP autorise les services de police et de gendarmerie, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, à inscrire dans un fichier les données recueillies dans deux cadres :
- d'une part, au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'État ;
- d'autre part, au cours des procédures de recherche des causes de la mort mentionnées à l'article 74 du CPP ou de recherche des causes d'une disparition mentionnées à l'article 74-1.

En application de l'article 230-7 du CPP, trois catégories de personnes sont susceptibles de voir leurs données personnelles inscrites dans un fichier d'antécédents judiciaires :
- les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées précédemment ;
- les victimes de ces infractions ;
- les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition.

À l'instar de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, concernant les anciens fichiers « système de traitement des infractions constatées » (STIC) et « système judiciaire de documentation et d'exploitation » (JUDEX), la loi du 14 mars 2011 a placé les fichiers de traitement des antécédents judiciaires, destinés à remplacer ces deux fichiers, sous le contrôle du procureur de la République territorialement compétent. Elle a cependant innové en confiant également ce contrôle à un « magistrat référent »1 doté des mêmes pouvoirs pour le suivi des données contenues dans les fichiers d'antécédents judiciaires (article 230-9 CPP). Les

personnes mises en cause peuvent donc s'adresser à deux magistrats différents pour obtenir la même décision.

Le texte renvoie à un décret le soin de fixer la durée de conservation des données.
Toutefois, il a prévu deux mécanismes d'effacement anticipé des données concernant les personnes mises en cause :

- un effacement de principe en cas de décision de relaxe ou d'acquittement devenue définitive, sauf si le procureur de la République ou le magistrat référent décide d'en prescrire le maintien « pour des raisons liées à la finalité du fichier » (cette formule a été modifiée par la loi du 3 juin 2016). Dans ce dernier cas, la décision doit faire l'objet d'une mention dans le fichier – ce qui exclut l'accès aux données personnelles dans le cadre d'enquêtes administratives – et la personne en est avisée ;
- une possibilité d'effacement en cas de décision de non-lieu ou de classement sans suite motivée par une insuffisance de charges (le périmètre de cette faculté a ensuite été étendu par la loi du 3 juin 2016 précitée). Contrairement au cas précédent, le principe est ici le maintien des données, assorti d'une mention au fichier (cette mention interdisant l'utilisation des données personnelles correspondantes dans le cadre d'enquêtes administratives), et l'exception l'effacement, discrétionnairement ordonné par le procureur de la République ou le magistrat référent.

Corrélativement, les personnes mises en cause dont les données ont été inscrites dans un fichier de traitement d'antécédents judiciaires se sont vues reconnaître la possibilité d'exiger une rectification en cas de requalification judiciaire. Cette rectification est de droit.

Pour les autres hypothèses d'inscription dans un fichier d'antécédents judiciaires, telles qu'une condamnation pénale ou un classement sans suite fondé sur un autre motif que l'insuffisance de charges, aucune possibilité expresse d'effacement anticipé n'avait en revanche été prévue à l'article 230-8 du CPP. Dans un avis rendu le 30 mars 20163, le Conseil d'État a cependant considéré que si l'effacement n'était pas possible dans le premier cas, il l'était malgré tout dans le second. En effet, le Conseil d'État a tout d'abord fait valoir que « *les dispositions de l'article 230-8 du code de procédure pénale […] ne prévoyant de règles particulières relatives au maintien ou à l'effacement des données du traitement des antécédents judiciaires qu'en cas de décisions de relaxe, d'acquittement, de non-lieu ou de classement sans suite, le législateur doit être regardé comme n'ayant entendu ouvrir la possibilité d'effacement que dans les cas où les poursuites pénales sont, pour quelque motif que ce soit, demeurées sans suite. Hors cette hypothèse, les données ne peuvent être effacées qu'à l'issue de la durée de conservation fixée par voie réglementaire et le procureur de la République ne peut alors que refuser une demande d'effacement avant ce terme* ». Puis, s'attachant au second cas, il a estimé que « Lorsque les faits à l'origine de l'enregistrement des données dont l'effacement est demandé ont fait l'objet d'un classement sans suite pour un autre motif que l'insuffisance de charges, les données sont assorties d'une mention et les dispositions précitées de l'article 230-8 du code de procédure pénale, si elles ne le prévoient pas expressément, ne font pas obstacle à ce que le procureur de la République ou le magistrat référent décide d'accueillir une demande d'effacement ».

Enfin, en application de l'article 230-10 du CPP : « *Les personnels spécialement habilités des services de la police et de la gendarmerie nationales désignés à cet effet ainsi que les personnels spécialement habilités de l'État investis par la loi d'attributions de police judiciaire, notamment les agents des douanes, peuvent accéder aux informations, y compris nominatives, figurant dans les traitements de données personnelles prévus par la présente section* », soit les fichiers d'antécédents judiciaires. Cet accès est également ouvert aux magistrats du parquet et aux magistrats instructeurs.

1.2. Application de l'article 230-8 dans le fichier « traitement des antécédents judiciaires »

Avant la loi du 14 mars 2011, des fichiers d'antécédents judiciaires étaient déjà utilisés par les services de police et de gendarmerie, mais leur existence était restée officieuse jusqu'à la fin des années 1990. L'officialisation intervint d'abord avec la création du STIC pour la police nationale et du JUDEX pour la gendarmerie nationale, qui donnèrent une assise réglementaire à ces fichiers de police, puis avec la loi du 18 mars 2003 précitée qui les dota d'une base légale.

À la suite de la LOPPSI, le STIC et le JUDEX ont été abrogés par le décret n° 2012-652 du 4 mai 2012 pour laisser place à un fichier commun aux services de police et de gendarmerie, dénommé « traitement des antécédents judiciaires » (TAJ), entré en vigueur le 31 décembre 2013.

Ce nouveau fichier, réglementé par les articles R. 40-23 et suivants du CPP, s'inscrit dans le cadre défini par les articles 230-6 à 230-9 du CPP. Ce fichier met ainsi en œuvre les finalités mentionnées à l'article 230-6 du CPP.

Le TAJ n'est toutefois pas seulement conçu comme un outil d'aide aux enquêtes judiciaires puisqu'il peut également être consulté dans le cadre des enquêtes administratives menées en vue de l'acquisition de la nationalité française et de la délivrance de titres pour les étrangers, de la promotion dans les ordres nationaux et de l'accès à certains emplois, notamment ceux participant à l'exercice des missions de souveraineté de l'État ou relevant du domaine de la sécurité ou de la défense.

Les informations susceptibles d'être collectées ainsi que leur durée de conservation varient en fonction des catégories d'individus en cause. Si l'on s'en tient aux seules personnes physiques mises en cause dans une affaire pénale, peuvent figurer au sein du TAJ : l'identité (nom – y compris le nom marital ou le nom d'emprunt officiel –, prénoms, surnom, sexe, date et lieu de naissance), la situation familiale, la filiation, la nationalité, les adresses postales, la profession, l'état de la personne, le signalement et toute photographie utile (article R. 40-26 CPP).

En mutualisant les anciens fichiers STIC et JUDEX, le TAJ a permis aux services de police et de gendarmerie de se doter d'une banque de données considérable puisqu'en 2015, la CNIL estimait à 9,5 millions le nombre de personnes enregistrées en qualité de « mises en cause ».

Les données concernant les individus majeurs mis en cause dans une affaire pénale sont conservées dans le TAJ pendant vingt ans, sous réserve des infractions pour lesquelles la durée est abaissée à cinq ans (tel est par exemple le cas du délit d'usage de stupéfiants) ou augmentée à

quarante ans. La durée de conservation des données concernant les mineurs est de cinq ans, sous réserve des infractions pour lesquelles elle peut atteindre dix, voire vingt ans

Les victimes d'infractions ne peuvent voir leurs données conservées pendant plus de quinze ans. Quant aux données concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition, elles doivent être effacées dès lors que l'enquête a permis de retrouver la personne disparue ou d'écarter toute suspicion de crime ou délit.

L'accès aux données contenues dans le TAJ pour les besoins des enquêtes judiciaires est ouvert en totalité aux acteurs investis par la loi d'attributions de police judiciaire. Dans le cadre d'enquêtes administratives, il est réservé à des personnels investis de missions de police administrative et ne permet pas l'accès aux données à caractère personnel se rapportant à des procédures judiciaires où sont intervenues des mesures ou décisions de classement sans suite, de non-lieu, de relaxe ou d'acquittement devenues définitives, ainsi que des données relatives aux victimes.

1.3. CADRE CONSTITUTIONNEL

Le cadre légal résultant de la LOPPSI a été jugé dans son ensemble conforme à la Constitution par le Conseil constitutionnel dans sa décision n° 2011-625 DC.

Le Conseil a notamment considéré que la différence de régime de conservation des données collectées à l'occasion d'une procédure ayant donné lieu à un classement sans suite, selon qu'un tel classement était motivé par une insuffisance de charges ou un autre motif, était justifiée par l'absence d'intérêt de conserver, dans le premier cas, de telles données dans le fichier.

Le Conseil s'est par ailleurs régulièrement prononcé sur des dispositions relatives à des traitements de données à caractère personnel, accessibles aux seules autorités administratives ou à des professionnels intéressés, notamment au regard du droit au respect de la vie privée qui découle de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 :.

Dans sa décision n° 2012-652 DC du 22 mars 2012, il a précisé ses exigences en matière de contrôle de fichiers en affirmant que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ». Il est ainsi passé, en matière de traitement de données, d'un contrôle limité à l'absence de disproportion manifeste à un contrôle de proportionnalité plus poussé.

Dans l'exercice de ce contrôle de proportionnalité, le Conseil constitutionnel tient notamment compte du nombre de personnes susceptibles de relever du fichier informatique en cause, de la sensibilité particulière des données personnelles recueillies, des garanties techniques ou juridiques prévues par le législateur et des finalités d'utilisation ou de consultation du fichier. C'est ce qui l'a conduit à censurer les dispositions instaurant un fichier d'identité biométrique portant sur la quasi-totalité de la population française, au motif que « compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées

dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire » (Décision n° 2012-652 DC).

Avant cette décision du 22 mars 2012, par laquelle il a précisé l'office de son contrôle en matière de traitements de données personnelles, le Conseil constitutionnel s'est prononcé à plusieurs reprises sur des fichiers de traitements d'antécédents judiciaires. Il a d'abord admis que les dispositions portant sur les traitements automatisés de données nominatives mis en œuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions prévoient un ensemble de garanties « de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée » (Décision n° 2003-467 DC du 13 mars 2003 précitée, cons. 21 à 27). Le Conseil a formulé comme seule réserve d'interprétation fondée sur le droit au respect de la vie privée la nécessité de garantir l'application de la loi du 6 janvier 1978 aux traitements en cause. Sans faire à proprement parler une réserve d'interprétation, le Conseil constitutionnel a par ailleurs relevé qu'il appartiendra à l'autorité judiciaire saisie d'une demande d'effacement « d'apprécier dans chaque cas, compte tenu des motifs de la décision prise, si les nécessités de l'ordre public justifient ou non le maintien des données en cause ». S'agissant de l'utilisation de ces fichiers à des fins administratives, il a par ailleurs jugé « qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées ».

Dans sa décision précitée n° 2011-625 DC, le Conseil constitutionnel a ensuite estimé, à propos des fichiers d'antécédents judiciaires, que « les modifications apportées aux dispositions de l'article 21 de la loi du 18 mars 2003 à l'occasion de leur introduction aux articles 230-6 à 230-11 du code de procédure pénale renforcent le contrôle de l'autorité judiciaire sur les données enregistrées dans les fichiers d'antécédents ; que l'article 230-8 du code de procédure pénale prévoit que le procureur de la République ou le magistrat chargé de suivre la mise en œuvre et la mise à jour des traitements se prononce, dans un délai d'un mois, sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification ; que cet article prévoit également que toutes les données relatives à des personnes mises en cause et maintenues dans les fichiers d'antécédents en dépit d'une décision de relaxe, d'acquittement, de non-lieu ou de classement sans suite, quel qu'en soit le motif, font l'objet d'une mention qui interdit l'accès à ces données dans le cadre d'une enquête administrative ; que la différence de régime de conservation des données, qui résulte de la faculté donnée au procureur de la République d'ordonner l'effacement lorsque le classement sans suite de la procédure est motivé par une insuffisance de charges, est fondée sur l'absence d'intérêt de conserver, dans ce cas, de telles données dans le fichier ; - […] qu'il résulte de ce qui précède que, sous les mêmes réserves que celles [formulées dans la décision n° 2003-467 DC], les dispositions des articles 230-6 à 230-11 du code de procédure pénale, qui ne sont ni obscures ni ambiguës, sont conformes à la Constitution ».

Dans cette même décision, au sujet des logiciels de rapprochement judiciaire, le Conseil constitutionnel a censuré la disposition permettant aux enquêteurs de prolonger, au-delà de trois ans, la conservation des données personnelles révélées par l'exploitation des enquêtes et des investigations réalisées au moyen de ces logiciels.

Le Conseil constitutionnel a par ailleurs eu l'occasion de se prononcer plus précisément sur des dispositions limitant les demandes d'effacement anticipé concernant les personnes mises en cause, à propos du FNAEG. Il a d'une part jugé que les garanties prévues par le législateur étaient de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée. Parmi les garanties relevées, il a notamment souligné « que l'inscription au fichier concerne, outre les personnes condamnées pour ces infractions, celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles les aient commises ; que, pour ces dernières, les empreintes prélevées dans le cadre d'une enquête ou d'une information judiciaires sont conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; qu'une procédure d'effacement est, dans ce cas, prévue par le législateur, lorsque la conservation des empreintes n'apparaît plus nécessaire compte tenu de la finalité du fichier ; que le refus du procureur de la République de procéder à cet effacement est susceptible de recours devant le juge des libertés et de la détention dont la décision peut être contestée devant le président de la chambre de l'instruction ».

Il a, d'autre part, considéré que le renvoi au décret pour fixer la durée de conservation des empreintes génétiques dans le FNAEG n'était pas contraire au principe de la présomption d'innocence, sous réserve notamment que le pouvoir réglementaire veille à « proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées ».

1.4 CADRE CONVENTIONNEL

Dans l'affaire Brunet contre France du 18 septembre 2014, la CEDH a jugé que la conservation pendant vingt ans, dans le STIC, des données d'un individu ayant bénéficié d'un classement sans suite pour un motif autre que l'insuffisance de charges était contraire au droit au respect de la vie privée garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDHLF), en raison de l'impossibilité pour l'autorité judiciaire d'ordonner l'effacement des données personnelles dans une telle hypothèse.

En réponse à ces décisions, l'article 68 de la loi n° 2016-731 du 3 juin 2016 a modifié l'article 230-8 du CPP afin, selon l'amendement présenté par le Gouvernement à cet effet, de « mettre le droit interne en conformité avec la jurisprudence de la CEDH ».

Désormais, le premier alinéa de l'article 230-8 prévoit que l'ensemble des décisions de classement sans suite peuvent donner lieu à un effacement anticipé des données figurant dans un traitement d'antécédents judiciaires, qu'elles soient ou non fondées sur une insuffisance de charges. Si le principe reste celui de la conservation des données assortie d'une mention de la décision dans le fichier, le procureur de la République ou le magistrat référent peut donc

apprécier, d'office ou sur la demande de l'intéressé, l'opportunité de les maintenir quel que soit le motif du classement sans suite.

*Le même alinéa précise ensuite que les décisions du procureur de la République ou du magistrat référent tendant au maintien ou à l'effacement des données sont prises pour des raisons liées à la finalité du fichier « au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé ».

L'article 230-8 ne limite ainsi plus l'exigence de motivation aux seules décisions de maintien des données en cas de relaxe ou d'acquittement définitifs.

Enfin, le troisième alinéa introduit un recours contre les décisions du procureur de la République devant le président de la chambre de l'instruction. Cette faculté est également ouverte contre les décisions du magistrat référent par le dernier alinéa de l'article 230-9, qui prévoit alors qu'elle s'exerce devant le président de la chambre de l'instruction de la cour d'appel de Paris.

2. OBJECTIFS ET NECESSITE DE LEGIFERER

2.1 OBJECTIFS POURSUIVIS

Le projet de loi réécrit le premier alinéa de l'article 230-8 afin de prévoir que les demandes d'effacement faites auprès du procureur de la République pourront intervenir sans délai à la suite d'une condamnation assortie d'une dispense de peine ou d'une dispense d'inscription au casier judiciaire, comme c'est déjà le cas pour les décisions de relaxe, d'acquittement, de non-lieu ou de classement sans suite, et qu'elles pourront intervenir dans les autres cas lorsqu'aucune mention ne figurera dans le bulletin n° du casier judiciaire.

Ainsi, dès qu'une condamnation sera réhabilitée ou non avenue, l'article 775 du code de procédure pénale prévoyant son exclusion du bulletin n° 2, la personne pourra demander l'effacement du TAJ des données la concernant, ou l'ajout à ces données d'une mention interdisant que le TAJ soit utilisé à des fins de police administrative.

2.2 NÉCESSITÉ DE LEGIFERER

Dans sa décisions n° 2017-670 QPC du 27 octobre 2017 du Conseil constitutionnel a déclaré contraire à la Constitution le premier alinéa de l'article 230-8 du code de procédure pénale, au motif que ces dispositions portaient une atteinte disproportionnée au droit au respect de la vie privée parce qu'elles privaient les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans ce fichier.

Après avoir déterminé la portée exacte des dispositions contestées, et avoir considéré qu'il résultait d'une jurisprudence constante qu'aucune personne mise en cause autre que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite ne peut obtenir, sur le fondement des dispositions contestées, l'effacement des données qui la

concernent » (paragr. 9), le Conseil constitutionnel a examiné leur conformité au droit au respect de la vie privée.

Comme il l'a fait dans de nombreuses décisions confrontant des dispositions relatives à un fichier aux exigences constitutionnelles en matière de vie privée, il a recherché les objectifs poursuivis par le législateur lors de la création de ce fichier. Sur ce point, il a jugé : « En autorisant la création de traitements de données à caractère personnel recensant des antécédents judiciaires et l'accès à ces traitements par des autorités investies par la loi d'attributions de police judiciaire et par certains personnels investis de missions de police administrative, le législateur a entendu leur confier un outil d'aide à l'enquête judiciaire et à certaines enquêtes administratives. Il a ainsi poursuivi les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public » (paragr. 9).

Le Conseil constitutionnel a ensuite apprécié le caractère proportionné à ces objectifs de l'atteinte à la vie privée résultant de l'inscription dans un fichier d'antécédents judiciaires.

Pour ce faire, il a d'abord examiné la nature des données pouvant être enregistrées dans un tel fichier, ainsi que le nombre de personnes susceptibles d'être inscrites dans le fichier. En effet, ces éléments entrent en ligne de compte dans la détermination de l'intensité de l'atteinte susceptible d'être portée à la vie privée.

Le Conseil a ainsi tout d'abord relevé que, « en prévoyant que les fichiers d'antécédents judiciaires peuvent contenir les informations recueillies au cours d'une enquête ou d'une instruction concernant une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer à la commission de certaines infractions, le législateur a permis que figurent dans ce fichier des données particulièrement sensibles » (paragr. 10).

À titre d'exemple, les dispositions réglementaires encadrant le TAJ prévoient ainsi que « peuvent être enregistrés, les éléments d'état civil, la profession ou la situation familiale de la personne, une photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale » (même paragr.).

Le Conseil constitutionnel a ensuite rappelé qu'un nombre important de personnes mises en cause dans une procédure pénale, et non pas seulement celles mises en cause pour les faits les plus graves, peuvent être inscrites dans un fichier d'antécédents judiciaires (paragr. 11).

Puis le Conseil constitutionnel a relevé l'absence, dans la loi, de durée maximum de conservation des informations enregistrées dans un fichier d'antécédents judiciaires. Le législateur a en effet renvoyé au pouvoir réglementaire la détermination de cette durée. Ainsi, l'article R. 40-27 du CPP prévoit qu'elles sont conservées pendant une durée comprise entre cinq ans et quarante ans, selon l'âge de l'individu et la nature de l'infraction (paragr. 12).

Enfin, dans l'appréciation de l'atteinte à la vie privée, le Conseil constitutionnel a pris en compte les cas dans lesquels ces fichiers peuvent être consultés : « ces informations peuvent être consultées non seulement aux fins de constatation des infractions à la loi pénale, de

rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative » (paragr. 13).

Après avoir mis ces éléments en balance, le Conseil constitutionnel en a conclu qu'« en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée » (paragr. 14).

Le Conseil constitutionnel a donc jugé que les personnes mises en cause dans une procédure pénale inscrites dans un fichier d'antécédents judicaires doivent pouvoir solliciter, et éventuellement obtenir, l'effacement de leurs données avant la fin de la durée normale de conservation. Il n'a pas pour autant reconnu « un droit à l'effacement », puisqu'il reviendra à l'autorité judiciaire d'apprécier le bien-fondé de cette demande, selon des critères définis par le législateur

Le Conseil a reporté les effets de sa décision au 1er mai 2018.

Cette décision impose de réécrire le premier alinéa de l'article 230-8 en respectant les exigences constitutionnelles, donc en prévoyant des possibilités d'effacement anticipé.

3. OPTIONS

3.1. DELAIS DANS LEQUEL UNE DEMANDE D'EFFACEMENT POURRA ETRE FORMEE

3.1.1. Option 1 (écartée) : Ne fixer aucun délai

Afin d'éviter une charge de travail excessive pour les parquets, il est proposé de ne pas permettre une possibilité immédiate de demande d'effacement (que n'exige du reste pas la décision QPC), sauf dans les cas déjà prévus de relaxe, acquittement, non-lieu et CSS, auxquels seraient ajoutés les cas de condamnations avec dispense de peine ou dispense d'inscription au casier.

3.1.2. Option 2 retenue : Prévoir un délai par référence à l'existence de mention au B2 du casier judiciaire

Dans cas autres que ceux de relaxe, acquittement, non-lieu, classement sans suite, et condamnations avec dispense de peine ou dispense d'inscription au casier., il est proposé de prévoir que la demande ne sera recevable que s'il n'existe plus de mention au B2 de la personne, ce qui est principalement le cas lorsque la condamnation est réhabilitée ou non avenue, et qu'elle disparaît donc du B2 en application des 4° et 5° de l'article 775 du CPP.

Cette solution paraît préférable à celle consistant à prévoir dans la loi un délai ou plusieurs délais spécifiques (alors que les délais de conservation dans le TAJ relèvent du décret). La référence au B2 est par ailleurs cohérente puisque le TAJ peut être utilisé à des fins administratives, comme le

B2 (et qu'il est parfois peu cohérent qu'une personne puisse se voir refuser un emploi en raison d'une mention au TAJ alors même que son B2 est néant).

Il résulte du renvoi aux règles du B2 pour permettre les demandes d'effacement du TAJ que les délais de recevabilité de ces demandes seront variables selon la nature des faits et de la peine prononcée (dans les cas les moins graves, notamment en cas de condamnation à une peine d'amende, ils seront de 3 ans après le paiement de celle-ci, conformément au 1° de l'article 133-13 du CP qui prévoit la réhabilitation de droit dans un tel délai ; dans les cas les plus graves de peines criminelles, ils seront au moins de 5 ans ou de 10 ans après l'exécution de la peine, selon qu'il y ou non récidive, en application des articles 786 et 787 du CPP, si la personne a obtenu une réhabilitation judiciaire ; il peut être précisé que ces délais ne s'appliquent qu'à la condition que la personne n'ait pas été de nouveau condamnée).

Le tableau figurant dans la partie impact précise les conséquences pratiques du renvoi aux règles du B2 du casier judiciaire.

3.2. NATURE DE LA DECISION POUVANT ETRE PRISE PAR LE PROCUREUR

3.2.1. Option 1 (écartée) : ne permettre au procureur que de décider d'effacer les données

Il aurait été incohérent de donner un seul pouvoir d'effacement au procureur, sans lui permettre de maintenir les données à des fins de police judiciaire, tout en les écartant des fins administratives..

3.2.2. Option 2 (retenue) : permettre au procureur d'ordonner l'effacement ou d'ordonner une mention

Il a logiquement été prévu que le procureur pourra décider de ne pas effacer les données du TAJ, mais d'ajouter une mention interdisant son utilisation à des fins administratives.

4. ANALYSE DES IMPACTS DE LA DISPOSITION ENVISAGÉE

4.1. IMPACTS JURIDIQUES

La présente disposition conduit à réécrire l'article 230-8 du code de procédure pénale.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

Les parquets pourront être plus fréquemment saisis de demande d'effacement concernant le TAJ

4.3. IMPACTS SUR LES PARTICULIERS

Les droits des personnes inscrites dans le TAJ seront augmentés, puisqu'elles pourront demander l'effacement des données avant les délais de conservations.

<table>
<tr><th colspan="2">REGLES D'INSCRIPTION ET D'EFFACEMENT DU BULLETIN N°2
et de possibilité de déposer une
REQUETE EN EFFACEMENT DU TAJ</th></tr>
<tr><td>Condamnés mineurs</td><td>Les condamnations pour mineurs ne sont jamais inscrites au bulletin n°2 du casier judiciaire (art 775 1° CPP).

En conséquence, les condamnés mineurs pourront solliciter immédiatement un effacement du TAJ.</td></tr>
<tr><td rowspan="2">Condamnés majeurs</td><td><u>En matière contraventionnelle :</u>

Les condamnations pour des contraventions de police ne sont jamais inscrites au bulletin n°2 du casier judiciaire (art 775 3° CPP).

En conséquence, les condamnés majeurs pourront solliciter immédiatement un effacement de la condamnation à une contravention de 5ème classe du TAJ</td></tr>
<tr><td><u>En matière correctionnelle :</u>

Toutes les condamnations correctionnelles, sauf celles prévues à l'article 706-47 CPP (nature sexuelle) peuvent faire au moment du prononcé de la décision, puis à tout moment sur requête de la personne condamnée l'objet d'une décision de non inscription ou d'exclusion du bulletin N°2 par la juridiction de jugement (art 775 2° et 775-1 CPP).
Si la décision est exclue ou effacée par la juridiction, la personne condamnée pourra logiquement solliciter son effacement du TAJ.
Hors de cette hypothèse, les condamnations correctionnelles sont effacées du bulletin n°2 dans les délais suivants :

<u>Déclaration de culpabilité assortie d'une dispense de peine ou d'un ajournement du prononcé de celle-ci :</u>
Ces condamnations ne sont pas inscrites au bulletin n°2 (art 775 12° CPP) et pourront donc faire l'objet d'une requête en effacement du TAJ immédiate.

<u>Amende :</u>
Les amendes sont effacées du bulletin n°2 à compter de leur réhabilitation légale (art 775 5° CPP), soit dans un délai de trois ans à compter du paiement (art 133-13 CP).

<u>Peines alternatives :</u>
Les jours-amende sont effacés du bulletin n°2 dans un délai de trois ans (art 775 11° CPP) à compter du caractère définitif de la condamnation.
Les autres peines alternatives prononcées sans sursis en application des articles 131-5 à 131-11 du code pénal sont effacés du bulletin n°2 dans un délai de cinq ans (art 775 11° CPP) à compter du caractère définitif de la condamnation.

<u>Peines d'emprisonnement assorties du sursis :</u>
Les condamnations assorties du sursis, avec ou sans mise à l'épreuve, sont effacées du bulletin n°2 lorsqu'elles sont considérées comme non avenues, (sauf suivi socio-judiciaire, interdiction d'exercer une activité en lien avec les mineurs, interdictions incapacités et déchéances prononcées à titre définitif, peine complémentaire d'inéligibilité qui persistent jusqu'en fin de mesure ou d'interdiction).

<u>Peines d'emprisonnement ferme réhabilitables :</u>
Les peines correctionnelles sont effacées du bulletin n°2 du casier judiciaire à</td></tr>
</table>

	compter de leur réhabilitation légale (art 775 5° CPP), laquelle intervient dans les délais suivants : - Emprisonnement inférieur ou égal à un an **: 5 ans** - Emprisonnement inférieur ou égal à 10 ans : **10 ans** - Emprisonnement résultant de peines multiples n'excédant pas 5 ans : **10 ans** Ces délais sont doublés si la personne est en état de récidive légale. Le délai court à compter de l'exécution ou de la prescription de la peine. <u>Peines d'emprisonnement ferme non réhabilitables :</u> Les peines d'emprisonnement correctionnelles suivantes ne sont pas susceptibles de réhabilitation de plein droit : - Emprisonnement supérieur à 10 ans - Emprisonnement résultant de peines multiples supérieur à 5 ans Lorsqu'elles n'ont pas été suivies d'une nouvelle condamnation à une peine criminelle ou correctionnelles, elles sont effacées dans un délai de **40 ans** (article 769 alinéa 3 CPP), sauf en cas de réhabilitation judiciaire, laquelle pouvant être sollicitée par sous certaines conditions dans un délai de 3 ans ou 6 en cas de récidive légale (art 786 et suivants CPP).
	<u>En matière criminelle :</u> Les peines criminelles ne peuvent pas être réhabilitées de plein droit. Ainsi, lorsqu'elles n'ont pas été suivies d'une nouvelle condamnation à une peine criminelle ou correctionnelles, elles sont effacées dans un délai de **40 ans** (article 769 alinéa 3 CPP), sauf en cas de réhabilitation judiciaire, laquelle pouvant être sollicitée par sous certaines conditions dans un délai de 5 ans ou 10 ans en cas de récidive légale (art 786 et suivants CPP).

5. CONSULTATION ET MODALITÉS D'APPLICATION

La Commission nationale de l'informatique et des libertés a été consultée.

La réforme s'appliquera dès le lendemain de la publication de la loi, en principe avant le 1er mai 2018, date à laquelle le Conseil constitutionnel a reporté l'application de sa décision de censure.

Aucun texte réglementaire ne doit être pris en application de la nouvelle rédaction de l'article 230-8 du code de procédure pénale.

Ces dispositions seront applicables sur l'ensemble du territoire, y compris dans les collectivités d'outre-mer. L'article « compteur » du code de procédure pénal est mis à jour en conséquence.

ARTICLES 24

1. L'article 24 du présent projet de loi précise la date d'entrée en vigueur des dispositions de la présente loi au 25 mai 2018. Il permet cependant, pour les traitements relevant de la directive, conformément à l'article 63 de celle-ci, un report de l'obligation de journalisation au 6 mai 2023 ou au 6 mai 2026.

Le projet de loi prévoit que les dispositions des titres I à III, ainsi que les articles 21et 22 entrent en vigueur à compter du 25 mai 2018, soit la date d'entrée en application du règlement (UE) 2016/679 (article 99).

L'article 63 de la directive (UE) 2016/680 prévoit quant à lui que : « 1. *Les États membres adoptent et publient, au plus tard le 6 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions. Ils appliquent ces dispositions à partir du 6 mai 2018.* ».

Ces deux textes qui font partie « du paquet européen de la protection des données », adoptés le même jour (27 avril 2016), sont donc applicables avec 19 jours de différence alors même qu'ils contiennent de très nombreuses dispositions en commun.

Ce décalage improbable vient peut-être du fait que la directive entre en vigueur le jour suivant celui de sa publication (article 64 de la directive) alors que le règlement entre en vigueur le vingtième jour suivant celui de sa publication (article 99 du règlement), soit 19 jours de différence également.

L'évolution du cadre de la protection des données du fait du règlement et de la directive est une source de complexité pour les acteurs privés et publics. Certaines dispositions spécifiques à la Commission nationale de l'informatique et des libertés s'appliquent peu importe les finalités du traitement.

Par conséquent, dans une optique de sécurité juridique et de simplification, le projet de loi prévoit une entrée en vigueur indifférenciée pour les titres Ier à III de la présente loi, à savoir le 25 mai 2018.

2. Sur les traitements en cours :

En ce qui concerne les traitements relevant du champ du règlement :

Le règlement est applicable à partir du 25 mai 2018. L'ensemble des traitements existants devront être conformes au règlement à cette date dès lors notamment que l'article 99 avait prévu une application deux ans après son adoption.

Le règlement a prévu le cas des accords conclus par les États membres. Son article 96 dispose en effet que : « *Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant le 24 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.* ».

Aucun autre article ne prévoit en revanche d'application différée pour les traitements relevant du règlement.

Le considérant 171 du règlement rappelle à cet égard l'obligation de mise en conformité : « *Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur.* ». Ce considérant prévoit cependant deux exceptions :

- D'une part, *« Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. »* ;
- D'autre part, *« Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées* ».

Ainsi, certains traitements mis en œuvre conformément au droit national antérieur au 25 mai 2018 pourront bénéficier de la présomption de conformité au règlement jusqu'à leur modification, remplacement ou abrogation, à savoir :

- les traitements ayant pour condition de licéité le consentement de la personne concernée, si le consentement a été donné dans les conditions prévues par le règlement. Toutefois, cette exception du consentement a une portée très limitée. Le considérant indique simplement qu'un traitement fondé sur le consentement reste valable si ce consentement a été donné dans les conditions du règlement, les autres règles de fond et de procédure du règlement ayant vocation à s'appliquer.

- les traitements soumis à certaines autorisations préalables de la Commission nationale de l'informatique et des libertés. Or ces autorisations semblent très limitées et il n'apparait pas que ce considérant puisse recouvrir les autorisations de l'article 25 de loi n° 78-17 ou les formalités préalables prévues par les articles 22 et 27 de cette même loi. L'article

46(5) du règlement semble, en effet, se limiter aux seules autorisations relatives à des transferts de données en dehors de l'Union européenne[147].

Toutefois, dans ses lignes directrices, le G29, groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données de l'Union européenne, donne une portée plus importante à ce considérant 171 du règlement : « *L'obligation d'effectuer une AIPD [analyse d'impact relative à la protection des données] s'applique aux opérations de traitement existantes susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.*

Aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, « Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées » *(considérant 171).*

À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en œuvre (portée, finalités, données à caractère personnel collectées, identité des responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'examen préalable effectué par l'autorité de contrôle ou le détaché à la protection des données et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD. (…)

À titre de bonne pratique, une AIPD devrait faire l'objet d'un examen continu et être régulièrement réévaluée. Par conséquent, même si une AIPD ne s'avère pas nécessaire le 25 mai 2018, il conviendra, le moment venu, que le responsable du traitement procède à une telle AIPD dans le cadre de ses obligations générales de responsabilité. »[148]

Le projet de loi ne prévoit pas une période de mise en conformité plus longue que celle prévue par le règlement, celle-ci devant s'entendre au regard du considérant 171.

En ce qui concerne les traitements relevant du champ de la directive :

---

[147] *« Les autorisations accordées par un État membre ou une autorité de contrôle sur le fondement de l'article 26, paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par ladite autorité de contrôle. Les décisions adoptées par la Commission sur le fondement de l'article 26, paragraphe 4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par une décision de la Commission adoptée conformément au paragraphe 2 du présent article. »*

[148] Groupe de travail « Article 29 » sur la protection des données ,« Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 » , version française, page 15 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

L'article 63 de la directive (UE) 2016/680 prévoit dans son § I que : *« Les États membres adoptent et publient, au plus tard le 6 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. (…). Ils appliquent ces dispositions à partir du 6 mai 2018. »*

Le § II indique cependant que : « *Par dérogation au paragraphe 1, un État membre peut prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant le 6 mai 2016 sont mis en conformité avec l'article 25, paragraphe 1, au plus tard le 6 mai 2023* ».

Le § 3 prévoit une dérogation plus importante aux § 1 et 2 en permettant « *dans des circonstances exceptionnelles* », la mise d'un système donné de traitement automatisé, en conformité avec l'article 25, paragraphe 1 « *dans un délai déterminé après le 6 mai 2023, sans que ce délai ne dépasse le 6 mai 2026 ; visé au paragraphe 2 du présent article, lorsque, à défaut de cela, de graves difficultés se poseraient pour le fonctionnement du système de traitement automatisé en question.* »

Le considérant 96 de la directive précise ces dispositions en indiquant que : « *Les États membres devraient disposer d'un délai maximal de deux ans à compter de la date d'entrée en vigueur de la présente directive pour sa transposition. Les traitements déjà en cours à cette date devraient être mis en conformité avec la présente directive dans un délai de deux ans après son entrée en vigueur. Toutefois, lorsque ces traitements ont lieu en conformité avec le droit de l'Union applicable avant la date d'entrée en vigueur de la présente directive, les exigences prévues par celle-ci concernant la consultation préalable de l'autorité de contrôle ne devraient pas s'appliquer aux opérations de traitement déjà en cours à ladite date, étant donné que ces exigences, de par leur nature même, doivent être satisfaites avant le traitement. Lorsque les États membres recourent au délai de mise en œuvre plus long, venant à expiration sept ans après la date d'entrée en vigueur de la présente directive, pour se conformer aux obligations en matière de journalisation pour les systèmes de traitement automatisé mis en place avant cette date, le responsable du traitement ou le sous-traitant devrait s'être doté des moyens effectifs de démontrer la licéité du traitement des données, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres »*

Toutefois, dans la mesure où sont maintenues les formalités préalables d'un arrêté ou d'un décret pris après avis de la Commission nationale de l'informatique et des libertés, les traitements valablement institués conformément à ces dispositions demeurent licites, même si des adaptations devront parfois être faites dans les textes réglementaires les ayant institué afin que ces textes soient mis en conformité avec les nouvelles dispositions législatives, mais que, même si ces adaptations ne sont pas réalisées avant la date butoir de transposition, cela ne rendra pas ces traitements illicites pour autant au regard du droit français.

La possibilité expresse, que propose l'article 28 du projet de loi, d'un report au 6 mai 2023, voire au 6 mai 2026, de l'obligation de journalisation prévue par l'article 25 de la directive ne doit en effet pas être interprétée comme impliquant que le 1 de l'article 63 de la directive prévoyant l'application des nouvelles dispositions à compter du 6 mai 2018 a pour conséquence de priver de base légale tous les traitements autorisés avant cette date.

3. La Commission nationale de l'informatique et des libertés a été consultée sur cet article.

ANNEXE

TABLEAU DE CONCORDANCE ENTRE LES DISPOSITIONS DE LA DIRECTIVE ET CELLES DE LA LOI DE 1978

(actuelles ou résultant du présent projet de loi)

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL Du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ***(les dispositions mentionnées en italique constituent soit des marges de manœuvre pour la transposition, soit des dispositions qui seront transposées par décret)***	**Droit interne en vigueur susceptible d'être modifié ou complété** (citation de la disposition concernée) Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ci-après dénommée « LIL » Décret n°2005-1309 du 20 octobre 2005 pris pour application de la loi 78-17 relative à l'informatique, aux fichiers et aux libertés	**Dispositions nouvelles résultant des articles 20 à 22 du projet de loi**	**Observations**

CHAPITRE I **DISPOSITIONS GÉNÉRALES** ***Article premier*** ***Objet et objectifs*** 1. La présente directive établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.		Le chapitre XIII de la même loi devient le chapitre XIV, et après l'article 70, il est inséré les dispositions suivantes : *CHAPITRE XIII.* ***DISPOSITIONS APPLICABLES AUX TRAITEMENTS RELEVANT DE LA DIRECTIVE (UE) 2016/680 DU 27 AVRIL 2016*** *Section 1.* ***Dispositions générales*** *Art. 70-1.* Les dispositions du présent chapitre s'appliquent, le cas échéant par dérogation aux autres dispositions de la présente loi, aux traitements des données à caractère personnel mis en œuvre : 1° A des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. 2° Par toute autorité publique compétente pour l'une des finalités énoncées au 1°, ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommée autorité compétente. Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour les finalités énoncées au 1°, par une autorité compétente au sens du 2°, et où sont respectées les dispositions des articles 70-3 et 70-4. Pour l'application du présent chapitre, lorsque les notions utilisées ne sont pas définies au chapitre premier de la présente loi, les définitions de l'article 4 du règlement (UE) 2016-679 sont applicables.	

2. Conformément à la présente directive, les États membres: a) protègent les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel; et b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis par le droit de l'Union ou le droit d'un État membre, ne soit ni limité ni interdit pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.	**Titre Ier : Dispositions communes** **Chapitre Ier : Principes et définitions** **Art 1er**. - L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.		Conforme
3. *La présente directive n'empêche pas les États membres de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes.*	**Maintien des Formalités préalables à la mise en œuvre des traitements concernés par la directive** **Article 26** I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat et: 1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. L'avis de la commission est publié avec l'arrêté autorisant le traitement. II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret	**Art. 70-3**. - Si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités prévues au 1° de l'article 70-1, il doit être prévu par un acte règlementaire pris conformément au I de l'article 26 et aux articles 28 à 31. Si le traitement porte sur des données mentionnées au I de l'article 8, il est prévu par un acte règlementaire pris conformément au II de l'article 26.	Cette disposition, combinée avec le considérant 15 de la directive, sert de fondement : Au maintien des formalités préalables à la mise en place d'un traitement en matière pénale, bien que non exigée par la directive, ces formalités représentant des garanties supplémentaires pour les droits des personnes concernées. Au maintien des dispositions impliquant que soit précisément déterminée la durée maximale de conservation des données dans un traitement, alors que la directive ne l'exige pas dès lors que la durée de conservation n'excède pas celle nécessaire aux finalités du traitement

	autorisant le traitement. III. - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission. IV. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation. **Article 30** I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent : 1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ; 2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions ; 3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;		

	4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ; 5° La durée de conservation des informations traitées ; 6° Le ou les services chargés de mettre en oeuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ; 7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ; 8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ; 9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ; 10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5. Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur		

	ces traitements doivent comporter au minimum. II. - Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la commission : - de tout changement affectant les informations mentionnées au I ; - de toute suppression du traitement. **Article 31** I. - La commission met à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26. Cette liste précise pour chacun de ces traitements : 1° L'acte décidant la création du traitement ou la date de la déclaration de ce traitement ; 2° La dénomination et la finalité du traitement ; 3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celles de son représentant ; 4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ; 5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ; 6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne. II. - La commission tient à la disposition du public ses avis, décisions ou recommandations. III. - La Commission		

	nationale de l'informatique et des libertés publie la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.		
Article 2 ***Champ d'application***			
1. La présente directive s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1.		Cf nouvel **article 70-1 susvisé**	
2. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.	**Art. 2**. La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.		Conforme
3. La présente directive ne s'applique pas au traitement de données à caractère personnel effectué: a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; b) par les institutions, organes, et organismes de l'Union.	**Article 41 LIL** Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient. La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. Lorsque la commission constate, en accord avec le responsable du traitement,		Maintien des dispositions actuelles de la LIL pour les traitements intéressant la sûreté de l'Etat et la défense qui ne relèvent pas du droit de l'Union. La disposition b) ne nécessite pas de transposition.

	que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.		
Article 3 ***Définitions***			
Aux fins de la présente directive, on entend par: 1."données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; 2. "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la	**Art. 2.** Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que	Cf nouvel **article 70-1 susvisé** **Article 70-1 2° susvisé -** Par toute autorité publique compétente pour l'une des finalités énoncées au 1°, ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommée autorité compétente. **Dernier alinéa de l'article 70-1 -** Pour l'application du présent chapitre, lorsque les notions utilisées ne sont pas définies au chapitre premier de la présente loi, les définitions de l'article 4 du règlement (UE) 2016-679 sont applicables.	Le droit français est conforme sur certaines définitions, telles que celles des données à caractère personnel, du traitement et du fichier. Les quelques variantes (comme les termes de structuration ou de limitation du traitement) restent de pure forme et sans conséquence sur le fond. Une transposition, dans le nouvelarticle et 70-1, est en revanche indispensable pour les définitions nouvelles qui ne figurent pas dans la loi informatique et libertés. Cet article opère un renvoi aux définitions identiques prévues par l'article 4 du règlement UE, et reproduit la définition propre à la directive de l'autorité compétente.

destruction; 3."limitation du traitement", le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur; 4. "profilage", toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne; 5. "pseudonymisation", le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable; 6."fichier", tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique; 7. "autorité compétente": a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou	le verrouillage, l'effacement ou la destruction. Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.		

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; 8."responsable du traitement", l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou le droit d'un État membre; 9. "sous-traitant", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ; 10. "destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement; 11. "violation de données à	**Art. 3. I-** Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. **Art. 3. II**- Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires. **Article 35 alinéa 2** - Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. **Article 34 bis**- I. - Le présent article s'applique au traitement des données à		

caractère personnel", une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données; 12."données génétiques", les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question; 13. "données biométriques", les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques; 14. "données concernant la santé", les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne; 15."autorité de contrôle", une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 41; 16. "organisation internationale",	caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification. Pour l'application du présent article, on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques. (…) **Art. 11.** La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations; 2° Elle veille à ce que les		

une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.	traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi (…).		

CHAPITRE II **PRINCIPES**			
Article 4 ***Principes relatifs au traitement des données à caractère personnel***			
1Les États membres prévoient que les données à caractère personnel sont: a)traitées de manière licite et loyale; b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ; c)adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées; d)exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder; e)conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; f)traitées de façon à garantir une sécurité appropriée des	**Art. 6**. Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : 1° Les données sont collectées et traitées de manière loyale et licite ; 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ; 4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour	***Section 2. - Obligations incombant aux autorités compétentes et aux responsables de traitements*** **Art. 70-11**. - Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 70-20. **Art. 70-20**. - I. - La personne concernée a le droit d'obtenir	Le droit français est conforme pour la plupart des dispositions. Le traitement sécurisé des données est assuré par le maintien des formalités préalables (cf art premier 3° de la directive), ainsi que par l'article 34 de la LIL. Des dispositions particulières sur la protection des données font par ailleurs l'objet d'une transposition (cf infra art. 19, 20 et 29 de la directive). La nécessité de rectification d'informations erronées « sans tarder » mentionnée au d) est transposée dans le nouvel article 70-11 pour les autorités compétentes, et à travers la notion de « meilleurs délais » reprise de l'article 16 de la directive dans l'article 70-20 s'agissant du responsable du traitement.

données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.	lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ; 5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. **Maintien des formalités préalables (cf art premier 3° directive), notamment l'article 30 LIL susvisé -** I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent : (…) 9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ; **Art. 34 premier alinéa** - Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. (…)	du responsable du traitement : 1° Que soit rectifiées dans les meilleurs délais des données à caractère personnel la concernant qui sont inexactes ; 2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ; 3° Que soit effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement. II. - Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier qu'il a procédé aux opérations exigées en vertu du I. (…)	
2. Le traitement, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 1*er*, paragraphe 1, autre que celles pour lesquelles les données ont été collectées, est autorisé à condition que: a) le responsable du	**Art. 6 susvisé** - **2°** [Les données à caractère personnel] sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.	**Art. 70-6**. - Les traitements effectués pour l'une des finalités énoncées au 1° de l'article 70-1 autre que celles pour lesquelles les données ont été collectées sont autorisés sous réserve du respect des principes prévus au chapitre I[er] de la présente loi et au présent chapitre.	

traitement soit autorisé à traiter ces données à caractère personnel pour une telle finalité conformément au droit de l'Union ou au droit d'un État membre; et b) le traitement soit nécessaire et proportionné à cette autre finalité conformément au droit de l'Union ou au droit d'un État membre. 3. Le traitement des données par le même ou par un autre responsable du traitement peut comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 1*er*, paragraphe 1, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.	Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; **Art. 36** actuel - Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en œuvre des traitements prévues au chapitre IV de la présente loi. Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa : -soit avec l'accord exprès de la personne concernée ou en vertu de ses directives, formulées dans les conditions définies à l'article 40-1 ; -soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ;	Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 70-1. **Art. 70-7.** - Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques sont mis en œuvre dans les conditions de l'article 36 de la présente loi. **Article 36 LIL modifié par l'article 12 du PJL** - Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa : -soit avec l'accord exprès de la personne concernée ou en vertu de ses directives, formulées dans les conditions définies à l'article 40-1 ; -soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article. Lorsque les traitements de données à caractère personnel sont mis en œuvre par les services publics d'archives à des fins archivistiques dans l'intérêt public conformément à l'article L. 211-2 du code du patrimoine, les droits visés aux articles 15, 16, 18, 19, 20 et 21 du règlement (UE) 2016/679 ne s'appliquent pas dans la mesure où ces droits rendent impossible ou entravent sérieusement la réalisation des finalités	

	-soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article.	spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités. Les conditions et garanties appropriées prévues à l'article 89 du règlement (UE) 2016/679 sont déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique.	
4. Le responsable du traitement est responsable du respect des paragraphes 1, 2 et 3 et est en mesure de démontrer que ces dispositions sont respectées.	**Art. 30 et 34 susvisés**	**Art 70-20 susvisé** **Art. 70-13**. - I. - Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable du traitement et le sous-traitant mettent en œuvre les mesures prévues aux paragraphes 1 et 2 de l'article 24 et aux paragraphes 1 et 2 de l'article 25 du règlement (UE) 2016/679 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8.	Cf également infra articles 19, 20, 29 de la directive.

Article 5 ***Délais de conservation et d'examen***			
Les États membres prévoient que des délais appropriés sont fixés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Des règles procédurales garantissent le respect de ces délais.	**Art. 6 susvisé** – 5° [Les données à caractère personnel] sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. **Article 30** I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent : (…); 5° La durée de conservation des informations traitées ; **Art. 36 susvisé -** Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. (…) **Art. L. 212-3 du code du patrimoine** - Lorsque les archives publiques comportent des données à caractère personnel collectées dans le cadre de traitements régis par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ces données font l'objet, à l'expiration de la durée prévue au 5° de l'article 6 de ladite loi, d'une sélection	**Art. 36 premier alinéa modifié par l'article 12 du PJL -** Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine.	Conforme L'article 30 de la LIL exige même que des durées maximales de conservation soient toujours déterminées.

	pour déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées. Les catégories de données destinées à l'élimination ainsi que les conditions de cette élimination sont fixées par accord entre l'autorité qui a produit ou reçu ces données et l'administration des archives. Lors des formalités préalables, il est par ailleurs prévu : **Art. 30 - I**. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent (…) 5° La durée de conservation des informations traitées ;		
Article 6 ***Distinction entre différentes catégories de personnes concernées***			
Les États membres prévoient que le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que: a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale; b) les personnes reconnues coupables d'une infraction pénale;		**Art. 70-12**. - Le responsable du traitement établit dans la mesure du possible et le cas échéant une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que: 1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale; 2° Les personnes reconnues coupables d'une infraction pénale; 3° Les victimes d'une	L'article 70-12 reprend intégralement les dispositions nouvelles de la directive.

c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale; et d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points a) et b).		infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale; 4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux 1° et 2°.	
Article 7 ***Distinction entre les données à caractère personnel et vérification de la qualité des données à caractère personnel***			
1. Les États membres prévoient que les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.		**Art. 70-8** - Les données à caractère personnel fondées sur des faits sont dans la mesure du possible distinguées de celles fondées sur des appréciations personnelles.	
2. Les États membres prévoient que les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à		***Section 2. - Obligations incombant aux autorités compétentes et aux responsables de traitements*** **Art. 70-11 susvisé**. - Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Dans la mesure du possible,	La LIL prévoit le droit pour la personne concernée de solliciter la mise à jour de ses données personnelles auprès du responsable du traitement, suivi le cas échéant d'une obligation pour ce dernier d'informer le tiers, à qui les données initiales avaient été transmises, de ces modifications. L'article 70-11 transpose donc l'obligation nouvelle expressément mise à la charge des autorités compétentes de veiller également à la qualité des données transmises, qui est prévue par la directive.

caractère personnel, et de leur niveau de mise à jour.		lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 70-20.	
3. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 16.	**Art. 40 alinéa 5 LIL susvisé** - Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa. ***Art. 99 décret*** *- Lorsque des données à caractère personnel ont été transmises à un tiers, le responsable du traitement qui a procédé à leur rectification en informe sans délai ce tiers. Celui-ci procède également sans délai à la rectification.*	**Dernier alinéa de l'article 70-11 susvisé** **Art. 70-20** V. Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont elles proviennent. VI. Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I, II et III, le responsable du traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.	
Article 8 ***Licéité du traitement***			
1. Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé		**Art. 70-1 susvisé** (avant-dernier alinéa) - Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour les finalités énoncées au 1°, par une autorité compétente au sens du 2°, et où sont	

sur le droit de l'Union ou le droit d'un État membre.		respectées les dispositions des articles 70-3 et 70-4.	
2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement.	Maintien des formalités préalables : **art 26, 28 à 31 LIL** (cf supra art premier 3° directive)	Cf art. 70-3 susvisé	
Article 9 ***Conditions spécifiques applicables au traitement***			
1. Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1*er*, paragraphe 1, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union ou le droit d'un État membre. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union. 2. Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1*er*, paragraphe 1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.		**Art. 70-5**. - Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées au 1° de l'article 70-1, ne peuvent être traitées pour d'autres finalités, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires, ou par le droit de l'Union européenne. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne. Lorsque les autorités compétentes sont chargées d'exécuter des missions autres que celles exécutées pour les finalités énoncées au 1° de l'article 70-1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne. Si le traitement est soumis à des conditions spécifiques, l'autorité compétente qui	Les « conditions spécifiques » sont explicitées dans le considérant 36 de la directive.

3. Les États membres prévoient que, lorsque le droit de l'Union ou le droit d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. 4. Les États membres prévoient que l'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dans lequel ladite autorité est établie.		transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. L'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dont relève l'autorité compétente qui transmet les données.	
Article 10 ***Traitement portant sur des catégories particulières de données à caractère personnel***			
Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement: a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre;	**Article 8 actuel** I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 1° Les traitements pour lesquels la personne concernée a donné son	**Art. 70-2**. - Le traitement de données mentionnées au I de l'article 8 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et, soit s'il est prévu par un acte législatif ou règlementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée. **Article 8 modifié par l'article 7 du PJL, notamment en ses I et IV** – I. Il est interdit de traiter des données à caractère personnel, qui	Par ailleurs, l'exigence d'un décret en Conseil d'Etat pour la création d'un traitement portant sur de telles données garantit la protection de ces données sensibles et la régularité du traitement (cf art. 70-3 susvisé).

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique; ou c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.	consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ; 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ; 3° Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical : - pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ; - sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ; - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ; 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ; 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ; 6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou	révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant vie sexuelle ou l'orientation sexuelle d'une personne physique. (…) *IV.* - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26.	

	de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ; 7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ; 8° Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX. III. Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions du chapitre IX ne sont pas applicables. IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les		

	conditions prévues au I de l'article 25 ou au II de l'article 26, soit déclarés dans les conditions prévues au V de l'article 22. **L'article 26 prévoit par ailleurs des formalités préalables particulières :** I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et : 1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. L'avis de la commission est publié avec l'arrêté autorisant le traitement. II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.(…)		
Article 11 ***Décision individuelle automatisée***			
1. Les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui fournit des garanties	**Art. 10. actuel** Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une	**Art. 70-9** - Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un	Le dernier alinéa de l'article 70-9 transpose le §3 de l'article 11 de la directive qui n'a pas d'équivalent dans la LIL. Les premier et deuxième alinéas de l'article 10 de la LIL ont été repris afin de ne pas réduire les droits existants et, dans un souci de lisibilité, afin de regrouper l'ensemble

appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. 2. Les décisions visées au paragraphe 1 du présent article ne sont pas fondées sur les catégories particulières de données à caractère personnel visées à l'article 10, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place. 3. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 est interdit, conformément au droit de l'Union.	personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.	traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 8 est interdit. **Art. 10 modifié par l'article 14 du PJL** : Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Outre les cas mentionnés aux *a* et *c* sous le 2 de l'article 22 du règlement 2016/679, aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée, à l'exception des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre I^{er} du titre I^{er} du livre IV du code des relations du public et de l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8. Pour les décisions administratives mentionnées à l'alinéa précédent, le responsable du traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions.	des dispositions relatives aux décisions individuelles prises sur le fondement d'un traitement automatisé de données personnelles.

CHAPITRE III **DROITS DE LA PERSONNE CONCERNÉE**			
Article 12 ***Communication et modalités de l'exercice des droits de la personne concernée***			
1. Les États membres prévoient que le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 13 et procède à toute communication relative au traitement ayant trait à l'article 11, aux articles 14 à 18 et à l'article 31 à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande. 2. Les États membres prévoient que le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par l'article 11 et les articles 14 à 18. 3. Les États membres prévoient que le responsable du traitement informe par écrit, dans les meilleurs délais, la personne concernée des suites données à sa demande. 4. Les États membres prévoient qu'aucun paiement n'est exigé pour fournir les informations visées à l'article 13 et pour procéder à toute communication et prendre toute mesure au titre de l'article 11, des articles 14 à 18 et de l'article 31. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le	**<u>LIL</u>** **Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes** **Section 2 : Droits des personnes à l'égard des traitements de données à caractère personnel.** **Article 38** Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement. **Article 39** I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;	**Art. 70-23** – Aucun paiement n'est exigé pour prendre les mesures et fournir les informations visées aux articles 70-18 à 70-20, sauf en cas de demande manifestement infondée ou abusive. Dans ce cas, le responsable du traitement peut également refuser de donner suite à la demande. En cas de contestation, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombe au responsable du traitement auprès duquel elles sont adressées.	Les droits de la personne (droit d'information prévu par l'article 13 de la directive, droit d'accès prévu par les articles 14 et 15, et droit de rectification ou d'effacement prévu par l'article 16) sont transposés dans les articles 70-18 à 70-24 (cf infra). Le droit d'information et le droit d'accès direct en matière pénale constituent les innovations principales de la directive. L'article 70-23 transpose, pour tous les droits, le principe de gratuité des informations fournies, avec la possibilité pour le responsable du traitement d'exiger le paiement de certains frais ou de s'opposer aux demandes manifestement abusives, à charge pour lui d'en rapporter la preuve. Les modalités de la réponse apportée à la demande par le responsable du traitement, qui doit faciliter l'exercice des droits (§1 à §3) seront précisées dans le décret d'application, à l'instar des éléments de vérification de l'identité de la personne concernée par les données (§5) déjà conformes dans le décret actuel.

responsable du traitement peut: a) soit exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder à la communication ou prendre les mesures demandées; b) soit refuser de donner suite à la demande. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande. 5. Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée à l'article 14 ou 16, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.	2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. II.-Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre,		

	leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées. Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés. **Article 40** I. — Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.		

	Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39. Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa. II. — Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci. En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation. Les deux premiers alinéas du présent II ne s'appliquent pas lorsque le traitement de données à caractère personnel est		

	nécessaire : 1° Pour exercer le droit à la liberté d'expression et d'information ; 2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; 3° Pour des motifs d'intérêt public dans le domaine de la santé publique ; 4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ; 5° A la constatation, à l'exercice ou à la défense de droits en justice. **DECRET** ***TITRE VI : DES OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENTS ET DES DROITS DES PERSONNES*** ***Chapitre Ier : L'obligation d'information incombant aux responsables de traitements*** ***(…)*** ***Art. 92****. - Les demandes tendant à la mise en œuvre des droits prévus aux articles 38 à 40 de la loi du 6 janvier 1978 susvisée, lorsqu'elles sont présentées par écrit au responsable du traitement, sont signées et accompagnées de la photocopie d'un titre d'identité portant la signature du titulaire. Elles précisent l'adresse à laquelle doit parvenir la réponse. Lorsqu'il existe un doute sur l'adresse indiquée ou sur l'identité du demandeur, la réponse peut être expédiée sous pli recommandé sans avis de réception, la vérification de l'adresse ou de l'identité du demandeur s'effectuant lors de la délivrance du pli.* ***Art. 93*** *- Lorsqu'une demande*		

	est présentée sur place, l'intéressé justifie par tout moyen de son identité auprès du responsable du traitement. Il peut se faire assister d'un conseil de son choix. La demande peut être également présentée par une personne spécialement mandatée à cet effet par le demandeur, après justification de son mandat, de son identité et de l'identité du mandant. *Lorsque la demande ne peut être satisfaite immédiatement, il est délivré à son auteur un avis de réception, daté et signé.* ***Art. 94** - Le responsable du traitement répond à la demande présentée par l'intéressé dans le délai de deux mois suivant sa réception.* *Si la demande est imprécise ou ne comporte pas tous les éléments permettant au responsable du traitement de procéder aux opérations qui lui sont demandées, celui-ci invite le demandeur à les lui fournir avant l'expiration du délai prévu à l'alinéa précédent. Le responsable du traitement y procède par lettre remise contre signature ou par voie électronique. La demande de compléments d'information suspend le délai prévu à l'alinéa précédent.* *Sauf lorsque la demande est manifestement abusive, les décisions du responsable du traitement de ne pas donner une suite favorable à la demande qui lui est présentée sont motivées et mentionnent les voies et délais de recours ouverts pour les contester.* *Le silence gardé pendant plus de deux mois par le responsable du traitement sur une demande vaut décision de refus.* *Lorsque le responsable du traitement ou, en application des articles 49 et 50, le correspondant à la protection des données n'est pas connu du*		

	demandeur, celui-ci peut adresser sa demande au siège de la personne morale, de l'autorité publique, du service ou de l'organisme dont il relève. La demande est transmise immédiatement au responsable du traitement. ***Art. 95*** *- Les codes, sigles et abréviations figurant dans les documents délivrés par le responsable de traitement en réponse à une demande doivent être explicités, si nécessaire sous la forme d'un lexique.* ***Art. 98*** *- La demande d'accès peut être effectuée par écrit.* *Lorsque le responsable du traitement permet la consultation des données sur place, celle-ci n'est possible que sous réserve de la protection des données personnelles des tiers. Sauf disposition législative ou réglementaire contraire, une copie des données à caractère personnel du demandeur peut être obtenue immédiatement.* *Afin que le demandeur puisse en prendre pleinement connaissance, le responsable de traitement met à la disposition de l'intéressé toutes les données qui le concernent et pendant une durée suffisante.* *Lors de la délivrance de la copie demandée, le responsable de traitement atteste, le cas échéant, du paiement de la somme perçue à ce titre.* ***Art. 100*** *- Outre la justification de son identité, l'héritier d'une personne décédée qui souhaite la mise à jour des données concernant le défunt doit, lors de sa demande, apporter la preuve de sa qualité d'héritier par la production d'un acte de notoriété ou d'un livret de famille.*		

Article 13 ***Informations à mettre à la disposition de la personne concernée ou à fournir à celle-ci***			
1. Les États membres prévoient que le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes: a) l'identité et les coordonnées du responsable du traitement; b) le cas échéant, les coordonnées du délégué à la protection des données; c) les finalités du traitement auquel sont destinées les données à caractère personnel; d) le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de ladite autorité; e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée. 2. En plus des informations visées au paragraphe 1, les États membres prévoient, par la loi, que le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits: a) la base juridique du traitement, b) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée; c) le cas échéant, les catégories de destinataires des	**L'article 32 de la LIL** qui fixe les informations devant être mis à disposition de la personne par le responsable de traitement **n'est pas applicable**, aux termes de son V « aux données recueillies dans les conditions prévues au III et **utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant** la sûreté de l'Etat, la défense, **la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté**, et aux termes de son VI, **« aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales »**. **Art. 32** I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ; 2° De la finalité poursuivie par le traitement auquel les données sont destinées ; 3° Du caractère obligatoire ou facultatif des réponses ; 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ; 5° Des destinataires ou catégories de destinataires des données ; 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à	**Article 18 du PJL** I. - A l'avant-dernier alinéa de l'article 32 de la même loi, les mots : « ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté » sont remplacés par les mots : « , sans préjudice de l'application des dispositions du chapitre XIII ». II. - Le dernier alinéa de l'article 32 est supprimé. (…) **Article 19 du PJL** ***Section 3. - Droits de la personne concernée*** ***Art. 70-18.*** – I. Le responsable du traitement met à la disposition de la personne concernée les informations suivantes: 1° l'identité et les coordonnées du responsable du traitement, et le cas échéant celles de son représentant; 2° le cas échéant, les coordonnées du délégué à la protection des données; 3° les finalités poursuivies par le traitement auquel les données sont destinées ; 4° le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission; 5° l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.	L'article 32 de la LIL n'étant pas applicable en matière pénale, le nouvel article 70-18 prévoit l'obligation nouvelle pour le responsable de traitement de mettre à disposition de la personne concernée certaines informations en matière pénale, créant ainsi un droit d'information en matière pénale. L'article 18 du projet de loi assure les coordinations nécessaires à l'article 32 de la loi du 6 janvier 1978 pour tirer les conséquences de ce nouveau droit à l'information.

données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales; d) au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.	caractère personnel après sa mort ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. (…) III.-Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données. Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.	II. - En plus des informations visées au I, le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits: 1° la base juridique du traitement, 2° la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ; 3° le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les Etats non membres de l'Union européenne ou au sein d'organisations internationales ; 4° au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.	

	(…) V.-Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement. VI.-Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.		
3. *Les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:* *a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;* *b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;* *c) protéger la sécurité publique;* *d) protéger la sécurité nationale;* *e) protéger les droits et libertés d'autrui.*		**Art. 70-21** I. Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article, dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne pour : 1° éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires; 2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; 3° protéger la sécurité publique ; 4° protéger la sécurité nationale ; 5° protéger les droits et libertés d'autrui. Ces restrictions sont prévues par l'acte instaurant le traitement. II. Lorsque les conditions prévues au I sont remplies, le responsable du traitement peut : 1° Retarder ou limiter la	La marge de manœuvre laissée aux Etats membres par la directive est transposée de manière générale pour tous les droits dans l'article 70-21 (cf infra). Celle prévue pour le droit d'information est ainsi transposée dans l'article 70-19 I et II 1°.

		fourniture à la personne concernée des informations mentionnées au II de l'article 70-18, ou ne pas fournir ces informations ; 2° Limiter, entièrement ou partiellement, le droit d'accès de la personne concernée prévu par l'article 70-19 ; 3° Ne pas informer la personne de son refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de cette décision conformément au IV de l'article 70-20. III. Dans les cas visés au 2° du II, le responsable du traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision, et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés. IV. En cas de restriction des droits de la personne concernée intervenue en application du II ou du III, le responsable du traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel.	
4. *Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, des points a) à e) du paragraphe 3.*			Pour les raisons précisées dans l'étude d'impact, le choix a été fait de ne pas faire usage de cette dérogation possible qui n'existe dans la directive que pour les droits d'information et d'accès.
Article 14 ***Droit d'accès par la personne***			

concernée			
Sous réserve de l'article 15, les États membres prévoient que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes: a) les finalités du traitement ainsi que sa base juridique; b) les catégories de données à caractère personnel concernées; c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales; d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée; e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée; f) le droit d'introduire une réclamation auprès de l'autorité de contrôle et les coordonnées de ladite autorité; g) la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.	**Art. 39 susvisé** I.- Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le	**Art. 70-19**. - La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes: 1° les finalités du traitement ainsi que sa base juridique ; 2° les catégories de données à caractère personnel concernées ; 3° les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des Etats non membres de l'Union européenne ou les organisations internationales ; 4° lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ; 5° l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement de ces données ; 6° le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission. 7° La communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.	

	coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. II.-Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées. Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés. ***Art. 98 décret susvisé*** *- La demande d'accès peut être effectuée par écrit.* *Lorsque le responsable du traitement permet la consultation des données sur place, celle-ci n'est possible que sous réserve de la protection des données personnelles des tiers. Sauf disposition législative ou réglementaire contraire, une copie des données à caractère personnel du demandeur peut être obtenue immédiatement.*		

	Afin que le demandeur puisse en prendre pleinement connaissance, le responsable de traitement met à la disposition de l'intéressé toutes les données qui le concernent et pendant une durée suffisante. *Lors de la délivrance de la copie demandée, le responsable de traitement atteste, le cas échéant, du paiement de la somme perçue à ce titre.*		
Article 15 ***Limitations du droit d'accès***			
1. Les États membres peuvent adopter des mesures législatives limitant, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour: *a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;* *b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;* *c) protéger la sécurité publique;* *d) protéger la sécurité nationale;* *e) protéger les droits et libertés d'autrui.*	**Art**. **41 LIL** - Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient. La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du	**Art. 18 du PJL** –(…) III. - A l'article 41 de la même loi, après les mots : « sécurité publique » sont insérés les mots : « , sous réserve de l'application des dispositions du chapitre XIII, ». IV. - A l'article 42 de la même loi, les mots : « prévenir, rechercher ou constater des infractions, ou de » sont supprimés. **Art. 70-21 susvisé** I. Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article, dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne pour : 1° éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires; 2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; 3° protéger la sécurité publique ; 4° protéger la sécurité nationale ; 5° protéger les droits et libertés d'autrui. Ces restrictions sont prévues par	La directive prévoyant un droit d'accès direct de principe en matière pénale, l'article 18 du PJL supprime l'exercice indirect des droits d'accès, de rectification et d'effacement des données prévu par l'article 42 de la loi actuelle pour les traitements intéressant la police judiciaire et ajoute une coordination nécessaire à l'article 41 de cette même loi pour les traitements intéressant la sécurité publique, la directive prévoyant par principe l'exercice direct de ces droits par la personne concernée auprès du responsable du traitement. L'article 70-21 I et II 2° transpose les possibilités de limitation du traitement prévues par la directive.

	fichier directement saisi. **Article 42 -** Les dispositions de l'article 41 sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions**,** ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27.	l'acte instaurant le traitement. II. Lorsque les conditions prévues au I sont remplies, le responsable du traitement peut : 1° Retarder ou limiter la fourniture à la personne concernée des informations mentionnées au II de l'article 70-18, ou ne pas fournir ces informations ; 2° Limiter, entièrement ou partiellement, le droit d'accès de la personne concernée prévu par l'article 70-19 ; 3° Ne pas informer la personne de son refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de cette décision conformément au IV de l'article 70-20. III. Dans les cas visés au 2° du II, le responsable du traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision, et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés. IV. En cas de restriction des droits de la personne concernée intervenue en application du II ou du III, le responsable du traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel.	
2. *Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements de données susceptibles de relever, dans leur intégralité ou en partie,*			Le choix a été fait de ne pas faire usage de cette dérogation possible, comme pour le droit d'information (Cf supra).

des points a) à e) du paragraphe 1.			
3. Dans les cas visés aux paragraphes 1 et 2, les États membres prévoient que le responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 1. Les États membres prévoient que le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.	***Art. 94 du décret*** *- Le responsable du traitement répond à la demande présentée par l'intéressé dans le délai de deux mois suivant sa réception.* *Si la demande est imprécise ou ne comporte pas tous les éléments permettant au responsable du traitement de procéder aux opérations qui lui sont demandées, celui-ci invite le demandeur à les lui fournir avant l'expiration du délai prévu à l'alinéa précédent. Le responsable du traitement y procède par lettre remise contre signature ou par voie électronique. La demande de compléments d'information suspend le délai prévu à l'alinéa précédent.* *Sauf lorsque la demande est manifestement abusive, les décisions du responsable du traitement de ne pas donner une suite favorable à la demande qui lui est présentée sont motivées et mentionnent les voies et délais de recours ouverts pour les contester.* *Le silence gardé pendant plus de deux mois par le responsable du traitement sur une demande vaut décision de refus.*	**Art. 70-21 III et IV susvisés**	La forme écrite de la réponse du responsable de traitement à la personne concernée sera précisée dans le décret d'application (cf supra article 12 directive).
4. Les États membres prévoient que le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition des autorités de contrôle.		**Art. 70-21 III susvisé**	.
Article 16 ***Droit de rectification ou d'effacement des données à caractère personnel et limitation du traitement***			
1. Les États membres prévoient le droit pour la personne concernée d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant	**Art. 40 susvisé** — Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la	**Art. 70-20** I. - La personne concernée a le droit d'obtenir du responsable du traitement : 1° Que soit rectifiées dans les meilleurs délais des données à caractère personnel la concernant	

qui sont inexactes. Compte tenu des finalités du traitement, les États membres prévoient que la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant à cet effet une déclaration complémentaire.	concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord. Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39. Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa. II. — Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers	qui sont inexactes ; 2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ; 3° Que soit effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement. II - Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier qu'il a procédé aux opérations exigées en vertu du I . III- Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque : 1° soit l'exactitude des données à caractère personnel est contestée par la personne concernée et il ne peut être déterminé si les données sont exactes ou non ; 2° soit les données à caractère personnel doivent être conservées à des fins probatoires. Lorsque le traitement est limité en vertu du 1°, le responsable du traitement informe la personne concernée avant de lever la limitation du traitement. IV. Le responsable du traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. V. Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont elles proviennent. VI. Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le	

	celles-ci, ou de toute copie ou de toute reproduction de celles-ci. En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation. Les deux premiers alinéas du présent II ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire : 1° Pour exercer le droit à la liberté d'expression et d'information ; 2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; 3° Pour des motifs d'intérêt public dans le domaine de la santé publique ; 4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ; 5° A la constatation, à l'exercice ou à la défense de droits en justice.	traitement a été limité au titre des I, II et III, le responsable du traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.	
2. Les États membres exigent que le responsable du traitement efface dans les meilleurs délais les données à caractère personnel et accordent à la personne concernée le droit d'obtenir du responsable du	**Art. 40 LIL** susvisé	**Art. 70-20 I et II susvisés**	

traitement l'effacement dans les meilleurs délais de données à caractère personnel la concernant lorsque le traitement constitue une violation des dispositions adoptées en vertu de l'article 4, 8 ou 10 ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.			
3. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque: a) l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non; ou b) les données à caractère personnel doivent être conservées à des fins probatoires. Lorsque le traitement est limité en vertu du premier alinéa, point a), le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.		**Art. 70-20 III susvisé**	
4. Les États membres prévoient que le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. *Les États membres peuvent adopter des mesures législatives limitant, en tout ou partie, l'obligation de fournir ces informations, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:* *a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;* *b) éviter de nuire à la prévention ou à la détection*		**Art. 70-20 IV et 70-21 susvisés**	L'article 70-21 I, II 3° et IV transpose les dispositions de l'article 16§4 de la directive, notamment les possibilités de limitation du traitement prévues par la directive.

d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales; *c) protéger la sécurité publique;* *d) protéger la sécurité nationale;* *e) protéger les droits et libertés d'autrui.* Les États membres prévoient que le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.			
5. Les États membres prévoient que le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont proviennent les données à caractère personnel inexactes. 6. Les Etats membres prévoient que, lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des paragraphes 1, 2 et 3, le responsable du traitement adresse une notification aux destinataires et que ceux-ci rectifient ou effacent les données à caractère personnel ou limitent le traitement des données à caractère personnel sous leur responsabilité.	**Art. 40 alinéa 5 LIL susvisé** - Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa. ***Art. 99 décret*** *- Lorsque des données à caractère personnel ont été transmises à un tiers, le responsable du traitement qui a procédé à leur rectification en informe sans délai ce tiers. Celui-ci procède également sans délai à la rectification.*	**Art. 70-20 V et VI susvisés** V. Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont elles proviennent. VI. Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I, II et III, le responsable du traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.	Cet article transpose l'obligation prévue par le §5 d'informer l'autorité compétente à l'origine de la transmission des données, et celle prévue par le §6 d'informer le destinataire.
Article 17 ***Exercice des droits de la personne concernée et vérification par l'autorité de contrôle***			
1. Dans les cas visés à l'article 13, paragraphe 3, à l'article 15, paragraphe 3, et à l'article 16, paragraphe 4, les États membres adoptent des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de	**Article 41 susvisé**	**Article 70-22** - En cas de restriction des droits de la personne concernée intervenue en application du II ou du III de l'article 70-21, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés.	

contrôle compétente.		Les dispositions des deuxième et troisième alinéas de l'article 41 sont alors applicables. Lorsque la commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires, elle l'informe également de son droit de former un recours juridictionnel.	
2. Les États membres prévoient que le responsable du traitement informe la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire de l'autorité de contrôle en application du paragraphe 1.		**Art. 70-21 IV susvisé**. En cas de restriction des droits de la personne concernée intervenue en application du II ou du III, le responsable du traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel.	
3. Lorsque le droit visé au paragraphe 1 est exercé, l'autorité de contrôle informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel.		**Art. 70-22 susvisé**	
Article 18 ***Droits des personnes concernées lors des enquêtes judiciaires et des procédures pénales***			
Les États membres peuvent prévoir que les droits visés aux articles 13, 14 et 16 sont exercés conformément au droit d'un État membre lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier ou dossier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale.		**Art 70-24** - Les dispositions de la présente sous-section ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données ne peut se faire que dans les conditions prévues par le code de procédure pénale.	

CHAPITRE IV **RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT**			
SECTION 1 **OBLIGATIONS GÉNÉRALES**			
Article 19 ***Obligations incombant au responsable du traitement***			
1. Les États membres prévoient que le responsable du traitement, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à la présente directive. Ces mesures sont réexaminées et actualisées, si nécessaire. 2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.	**Maintien des formalités préalables : art. 26 à 31 LIL susvisés.** **Art. 34** Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.	**Art. 70-13.** - I. - Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable du traitement et le sous-traitant mettent en œuvre les mesures prévues aux paragraphes 1 et 2 de l'article 24 et aux paragraphes 1 et 2 de l'article 25 du règlement (UE) 2016/679 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8. II- En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à : 1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ; 2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ; 3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection,	L'article 70-13, qui reprend des dispositions issues des articles 19, 20, 22§1 et 29 de la directive (cf infra), précisent et complètent les dispositions de l'article 34 de la LIL relatif aux mesures à mettre en œuvre pour assurer la sécurité des données.

		la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ; 4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ; 5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ; 6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ; 7° Garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction); 8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ; 9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ; 10° Garantir que les fonctions du système opèrent, que les	

		erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).	
Article 20 ***Protection des données dès la conception et protection des données par défaut***			
1. Les États membres prévoient que, compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant lors de la détermination des moyens du traitement que lors du traitement proprement dit, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires, afin de répondre aux exigences de la présente directive et de protéger les droits des personnes concernées. 2. Les États membres prévoient que le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes	**Art. 34 susvisé** ***Art. 91-3 du décret*** *Constitue une mesure de protection appropriée, au sens de l'article 34 bis de la loi du 6 janvier 1978, toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.*	**Art. 70-13 I susvisé**	

physiques sans l'intervention de la personne concernée.			
Article 21 ***Responsables conjoints du traitement***			
1. Les États membres prévoient que, lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect de la présente directive, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées à l'article 13, par voie d'accord entre eux, sauf si et dans la mesure où leurs obligations respectives sont définies par le droit de l'Union ou le droit d'un État membre auquel les responsables du traitement sont soumis. Le point de contact pour les personnes concernées est désigné dans l'accord. Les États membres peuvent préciser lequel des responsables conjoints peut servir de point de contact unique pour que les personnes concernées puissent exercer leurs droits. *2. Indépendamment des termes de l'accord visé au paragraphe 1, les États membres peuvent prévoir que la personne concernée peut exercer les droits que lui confère les dispositions adoptées en vertu de la présente directive à l'égard de et contre chacun des responsables du traitement.*			Ces dispositions seront transposées par décret. Excepté la marge de manœuvre de la dernière phrase du 1°, ces dispositions sont identiques à celles de l'article 26 du règlement.

Article 22 ***Sous-traitant***			
1. Les États membres prévoient que le responsable du traitement, lorsqu'un traitement doit être effectuée pour son compte, fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la présente directive et garantisse la protection des droits de la personne concernée. 2. Les États membres prévoient que le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements. 3. Les États membres prévoient que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant: a) n'agit que sur instruction du responsable du traitement; *b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de*	**Art. 35** - Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.	**Art. 70-10**. - Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant que dans les conditions prévues aux paragraphes 1, 2, 9 et 10 de l'article 28 et à l'article 29 du règlement (UE) 2016/679 et au présent article. Les sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent chapitre et garantisse la protection des droits de la personne concernée. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement, et qui prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement. Le contenu de ce contrat ou acte juridique est précisé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.	L'article 70-10 vient compléter l'article 35 de la LIL afin de transposer les dispositions nouvelles relatives au sous-traitant. Les précisions relatives au contenu du contrat entre le responsable du traitement et le sous-traitant figureront dans le décret d'application.

confidentialité; *c) aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée;* *d) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation des services de traitement des données, et détruit les copies existantes, à moins que le droit de l'Union ou le droit d'un État membre n'exige la conservation des données à caractère personnel;* *e) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect du présent article;* *f) respecte les conditions visées aux paragraphes 2 et 3 pour recruter un autre sous-traitant.* 4. Le contrat ou l'autre acte juridique visé au paragraphe 3 revêt la forme écrite, y compris la forme électronique. 5. Si, en violation de la présente directive, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.			
Article 23 ***Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant***			
Les États membres prévoient que le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite que sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre.	**Art. 35 susvisé** Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. (…) Le contrat liant le sous-traitant au responsable du traitement	**Art. 70-10 susvisé**	L'article 23 de la directive est transposé par le renvoi à l'article 29 du règlement.

	comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.		
Article 24 ***Registre des activités de traitement***			
1. Les États membres prévoient que les responsables du traitement tiennent un registre de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes: a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement et du délégué à la protection des données; b) les finalités du traitement; c) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales; d) une description des catégories de personnes concernées et des catégories de données à caractère personnel; e) le cas échéant, le recours au profilage; f) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale; g) une indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées; h) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données à caractère personnel; i) dans la mesure du		**Art. 70-14**.- Le responsable du traitement et le sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux paragraphes 1 à 4 de l'article 30 du règlement (UE) 2016/679. Ce registre contient aussi la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.	

possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 29, paragraphe 1.			
2. Les États membres prévoient que chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant: a) le nom et les coordonnées du ou des sous-traitants, de chaque responsable du traitement pour le compte duquel le sous-traitant agit et, le cas échéant, du délégué à la protection des données; b) les catégories de traitements effectués pour le compte de chaque responsable du traitement; c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, lorsqu'il en est expressément chargé par le responsable du traitement, y compris l' identification de ce pays tiers ou de cette organisation internationale; d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 29, paragraphe 1.		**Art. 70-14 susvisé**	
3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite, y compris la forme électronique. Le responsable du traitement et le sous-traitant mettent ces registres à la disposition de l'autorité de contrôle, sur demande.		**Art 70-14 susvisé**	

Article 25 ***Journalisation***			
1. Les États membres prévoient que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel. 2. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales. 3. Le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle, sur demande.		**Art. 70-15**. **-** Le responsable du traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation, de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données. Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et leurs destinataires. Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales. Ce journal est mis à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.	
Article 26 ***Coopération avec l'autorité de contrôle***			
Les États membres prévoient que le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.		**Art. 70-16**. - Les articles 31, 33 et 34 du règlement (UE) 2016/679 sont applicables aux traitements des données à caractère personnel relevant du présent chapitre.	Mise en conformité avec l'article 26 de la directive par le renvoi à l'article 31 du règlement.

Article 27 ***Analyse d'impact relative à la protection des données***			
1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. 2. *L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.*		**Art. 70-4.** - Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable du traitement effectue une analyse d'impact relative à la protection des données à caractère personnel. Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue par l'article 30. Dans les autres cas, le responsable du traitement ou le sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement au traitement des données à caractère personnel : 1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; 2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.	Le contenu de l'analyse d'impact sera précisé dans le décret.

Article 28 ***Consultation préalable de l'autorité de contrôle***			
1. Les États membres prévoient que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer: a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 27, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. 2. Les États membres prévoient que l'autorité de contrôle est consultée dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui se rapporte au traitement. 3. Les États membres prévoient que l'autorité de contrôle peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1. 4. Les Etats membres prévoient que le responsable du traitement fournit à l'autorité de contrôle l'analyse d'impact relative à la protection des données en vertu de l'article 27 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.	Maintien des formalités préalables : **art. 26, et 28 à 31 LIL** susvisés	**Art. 70-4 susvisé** **Article 1er du PJL** L'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié : (…) 9° Après le *h* du 2°, il est inséré un *i* ainsi rédigé : *i)* Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 » ; (…)	

5. Les États membres prévoient que, lorsque l'autorité de contrôle est d'avis que le traitement prévu, visé au paragraphe 1 du présent article, constituerait une violation des dispositions adoptées en vertu de la présente directive, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement , et le cas échéant au sous-traitant, et elle peut faire usage des pouvoirs visés à l'article 47. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement prévu. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.			
SECTION 2 **SÉCURITÉ DES DONNÉES**			
Article 29 ***Sécurité du traitement***			
1. Les États membres prévoient que, compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 10.	**Art. 8 et 34 LIL susvisés** ***Art. 91-3 décret susvisé***	**Art. 70-13 I susvisé** - I. - Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable du traitement et le sous-traitant mettent en œuvre les mesures prévues aux paragraphes 1 et 2 de l'article 24 et aux paragraphes 1 et 2 de l'article 25 du règlement (UE) 2016/679 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8.	

2. En ce qui concerne le traitement automatisé, chaque État membre prévoit que le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à: a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations); b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données); c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation); d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs); e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données); f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission); g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);		**Art. 70-13 II susvisé** – II- En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à : 1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ; 2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ; 3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ; 4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ; 5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ; 6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ; 7° Garantir qu'il puisse être vérifié et constaté a posteriori	Transposition des prescriptions particulières prévues pour les traitements automatisés par l'article 29 §2 de la directive.

h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport); i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration); j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).		quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction); 8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ; 9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ; 10° Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).	
Article 30 ***Notification à l'autorité de contrôle d'une violation de données à caractère personnel***			
1. Les États membres prévoient qu'en cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question à l'autorité de contrôle dans les meilleurs délais *et, si possible, dans un délai de 72 heures au plus tard après en avoir pris connaissance*, à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et les libertés d'une personne physique. *Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.* 2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais	**Art. 34 bis** I. - Le présent article s'applique au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification. Pour l'application du présent article, on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou	**Art. 70-16. -** Les articles 31, 33 et 34 du règlement (UE) 2016/679 sont applicables aux traitements des données à caractère personnel relevant du présent chapitre. Si la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre Etat membre ou à celui-ci, le responsable du traitement notifie également la violation au responsable du traitement de l'autre Etat membre dans les meilleurs délais. La communication d'une violation de données à	L'article 70-16 transpose les articles 30 et 31 de la directive qui sont quasiment identiques aux articles 33 et 34 du règlement, la notification des violations de sécurité n'existant à l'article 34bis de la loi actuelle que pour les fournisseurs de services électroniques en ligne.

après en avoir pris connaissance.	l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques. II. - En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés. Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé. La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation. A défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés. III. - Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission. ***Article 91-1 décret*** *La notification d'une violation des données à caractère*	caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, lorsque sa mise en œuvre est de nature à mettre en danger la sécurité publique, la sécurité nationale ou les droits ou libertés d'autrui ou à faire obstacle au bon déroulement des enquêtes et procédures destinées à prévenir, détecter ou poursuivre des infractions pénales ou à exécuter des sanctions pénales. **Art. 70-16 susvisé**	

	personnel prévue au premier alinéa du II de l'article 34 bis de la loi du 6 janvier 1978 susvisée est adressée à la Commission nationale de l'informatique et des libertés par lettre remise contre signature qui précise la nature et les conséquences de la violation des données à caractère personnel, les mesures déjà prises ou proposées par le fournisseur de services de communications électroniques accessibles au public pour y remédier et les personnes auprès desquelles des informations supplémentaires peuvent être obtenues et, lorsque cela est possible, une estimation du nombre de personnes susceptibles d'être impactées par la violation en cause. ***Art. 91-4 décret*** *Pour informer la Commission nationale de l'informatique et des libertés des mesures de protection qu'il met en œuvre et qu'il a appliquées au cas particulier, le fournisseur lui adresse, par tout moyen permettant d'apporter la preuve de leur notification, les informations suivantes :* *1° Les nom, prénom, adresse et coordonnées téléphoniques du responsable du traitement ;* *2° La description des mesures de protection ;* *3° Les dispositions prévues et appliquées pour conférer une pleine efficacité à ces mesures ;* *4° Le cas échéant, les références du dossier de formalités accomplies auprès de la commission préalablement à la mise en œuvre du traitement considéré ;* *5° L'accomplissement ou non de la formalité de notification prévue à la personne intéressée par l'article 91-2 et, dans la négative, les raisons justifiant l'absence de notification.* ***Art. 91-5 décret*** *La Commission nationale de l'informatique et des libertés vérifie dans un délai de deux mois si les mesures de*		

	protection appropriées ont été mises en œuvre et appliquées et apprécie la gravité au cas particulier de la violation de données à caractère personnel. *Le silence gardé par la commission au terme de ce délai vaut constat de non-application au cas particulier des mesures de protection appropriées et emporte pour le fournisseur, s'il n'a pas déjà averti la personne intéressée, l'obligation de procéder à la notification prévue à l'article 91-2. Ce délai ne court qu'à compter de la réception complète des informations prévues à l'article 91-4.* *Si le fournisseur n'a pas déjà averti la personne intéressée de la violation de ces données en application de l'article 91-2, la commission peut en outre, lorsqu'elle estime la violation grave, mettre le fournisseur en demeure de l'informer en application du dernier alinéa du II de l'article 34 bis de la loi du 6 janvier 1978 dans un délai qui ne peut être supérieur à un mois.*		
3. La notification visée au paragraphe 1 doit, à tout le moins: a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés; b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues; c) décrire les conséquences probables de la violation de données à caractère personnel; d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à			

la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. 4. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu. 5. Les États membres prévoient que le responsable du traitement documente toute violation de données à caractère personnel visée au paragraphe 1, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article. 6. Les États membres prévoient que, lorsque la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre ou à celui-ci, les informations visées au paragraphe 3 sont communiquées au responsable du traitement de cet État membre dans les meilleurs délais.			
Article 31 ***Communication à la personne concernée d'une violation de données à caractère personnel***			
1. Les États membres prévoient que, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne physique, le responsable du traitement communique la violation à la personne concernée dans les meilleurs délais. 2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations	**Art. 34 bis II susvisé** ***Article 91-2 décret*** *La notification d'une violation des données à caractère personnel prévue au deuxième alinéa du II de l'article 34 bis de la loi du 6 janvier 1978 est adressée à la personne intéressée par tout moyen permettant au fournisseur de services de communications électroniques accessibles au public d'apporter la preuve de l'accomplissement de cette formalité. Cette notification précise la nature de la violation*	**Art. 70-16 susvisé**	

et les recommandations prévues à l'article 30, paragraphe 3, points b), c) et d). 3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie: a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces dernières ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement; b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et les libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser; c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. 4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie. 5. La communication à la personne concernée visée au paragraphe 1 du présent article peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 13, paragraphe 3.	*de données à caractère personnel, les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ainsi que les mesures que le fournisseur recommande à la personne intéressée de prendre pour atténuer les conséquences négatives de cette violation.* *Cette notification n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que les mesures de protection appropriées au sens de l'article 91-3 et sur lesquelles elle s'est prononcée dans les conditions prévues aux articles 91-4 et 91-5 ont été mises en œuvre par le fournisseur et efficacement appliquées aux données concernées par cette violation.* ***Art. 91-4 et 91-5 décret suvisés***		

SECTION 3 **DÉLÉGUÉ À LA PROTECTION DES DONNÉES**			
Article 32 ***Désignation du délégué à la protection des données***			
1. Les États membres prévoient que le responsable du traitement désigne un délégué à la protection des données. Les États membres peuvent dispenser les tribunaux et d'autres autorités judiciaires indépendantes de cette obligation lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle. 2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à exercer les missions visées à l'article 34. 3. Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille. 4. Les États membres prévoient que le responsable du traitement publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle.	.	**Art. 70-17**. I- Sauf pour les juridictions agissant dans l'exercice de leur fonction juridictionnelle, le responsable du traitement désigne un délégué à la protection des données. Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille. Les dispositions des paragraphes 5 et 7 de l'article 37, des paragraphes 1 et 2 de l'article 38 et du paragraphe 1 de l'article 39 du règlement (UE) 2016/679, en ce qu'elles concernent le responsable du traitement, sont applicables aux traitements des données à caractère personnel relevant du présent chapitre.	
Article 33 ***Fonction du délégué à la protection des données***			
1. Les États membres prévoient que le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. 2. Le responsable du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 34 en		**Art. 70-17 susvisé**	

fournissant les ressources nécessaires pour exercer ces missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permettant d'entretenir ses connaissances spécialisées.			
Article 34 ***Missions du délégué à la protection des données***			
Les États membres prévoient que le responsable du traitement confie au délégué à la protection des données au moins les missions suivantes: a) informer et conseiller le responsable du traitement et les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la présente directive et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données; b) contrôler le respect de la présente directive, d'autres dispositions du droit de l'Union ou du droit États membres en matière de protection des données et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant à des opérations de traitement, et les audits s'y rapportant; c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 27; d) coopérer avec l'autorité de contrôle; e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 28, et mener des consultations, le cas échéant, sur tout autre sujet.		**Art. 70-17 susvisé**	

CHAPITRE V ***Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales*** ***Article 35*** **Principes généraux applicables aux transferts de données à caractère personnel** 1. Les États membres prévoient qu'un transfert, par des autorités compétentes, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après leur transfert vers un pays tiers ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays tiers ou à une autre organisation internationale, n'a lieu, sous réserve du respect des dispositions nationales adoptées en application d'autres dispositions de la présente directive, que lorsque les conditions définies dans le présent chapitre sont respectées, à savoir: a)le transfert est nécessaire aux fins énoncées à l'article 1er, paragraphe 1; b)les données à caractère personnel sont transférées à un responsable du traitement dans un pays tiers ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 1er, paragraphe 1; c)en cas de transmission ou de mise à disposition de données à caractère personnel provenant d'un autre État membre, celui-ci a préalablement autorisé ce transfert conformément à son droit national; d)la Commission a adopté une décision d'adéquation en application de l'article 36, ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 37 ou, en l'absence de décision d'adéquation au titre de l'article 36 et de garanties appropriées conformément à	**Article 68 LIL** Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. **Article 69** Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes : 1° A la sauvegarde de la vie de cette personne ; 2° A la sauvegarde de l'intérêt public ;	**Art. 70-25**. - Le responsable d'un traitement de données à caractère personnel ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées : 1° Le transfert de ces données est nécessaire à l'une des finalités énoncées au 1° de l'article 70-1 ; 2° Les données à caractère personnel sont transférées à un responsable dans cet État tiers ou à une organisation internationale qui est une autorité compétente chargée dans cet État des fins relevant en France du 1° de l'article 70-1 ; 3° Si les données à caractère personnel proviennent d'un autre État, l'État qui a transmis ces données a préalablement autorisé ce transfert conformément à son droit national. Toutefois, si l'autorisation préalable ne peut pas être obtenue en temps utile, ces données à caractère personnel peuvent être retransmises sans l'autorisation préalable de l'État qui a transmis ces données lorsque cette retransmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre État ou pour la sauvegarde des intérêts essentiels de la France. L'autorité d'où provenaient ces données personnelles est informée sans	

l'article 37, des dérogations pour des situations particulières s'appliquent en vertu de l'article 38; et e)en cas de transfert ultérieur vers un autre pays tiers ou à une autre organisation internationale, l'autorité compétente qui a procédé au transfert initial ou une autre autorité compétente du même État membre autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement. 2. Les États membres prévoient que les transferts effectués sans l'autorisation préalable d'un autre État membre prévue au paragraphe 1, point c), sont autorisés uniquement lorsque le transfert de données à caractère personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans retard. 3. Toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques assuré par la présente directive ne soit pas compromis.	3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ; 4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ; 5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ; 6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'Etat pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet. La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel qu'elle	retard. 4° L'une au moins des trois conditions suivantes est remplie : *a)* La Commission a adopté une décision d'adéquation en application de l'article 36 de la directive (UE) 2016/680 du Parlement et du Conseil du 27 avril 2016 ; *b)* A défaut d'une telle décision d'adéquation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ; ces garanties appropriées peuvent soit résulter des garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet État tiers, soit résulter de dispositions juridiquement contraignantes exigées à l'occasion de l'échange de données ; *c)* A défaut d'une telle décision d'adéquation et de garanties appropriées telles que prévues au *b*, le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel ; Lorsque le responsable d'un traitement de données à caractère personnel transfère des données à caractère personnel sur le seul fondement de l'existence de garanties appropriées au regard de la protection des données à caractère personnel, autre qu'une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles, il avise la Commission nationale de l'informatique et des libertés des catégories de transferts relevant de ce fondement. Dans ce cas, le responsable du traitement des données doit	

	prend au titre de l'alinéa précédent.	garder trace de la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et des données à caractère personnel transférées. Cette documentation est mise à la disposition de l'autorité de contrôle, sur sa demande. Lorsque la commission a abrogé, modifié ou suspendu une décision d'adéquation adoptée en application de l'article 36 de la directive précitée, le responsable d'un traitement de données à caractère personnel peut néanmoins transférer des données personnelles ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ou s'il estime après avoir évalué toutes les circonstances du transfert qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.	
Article 36 **Transferts sur la base d'une décision d'adéquation** 1. Les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.			
2. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte en particulier des éléments suivants: a)l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation			Dispositions concernant la Commission et n'ayant pas lieu d'être transposées dans la législation française.

pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées;			
b)l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres; et			
c)les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants et de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel. 3. La Commission, après avoir			

évalué le caractère adéquat du niveau de protection, peut constater au moyen d'un acte d'exécution qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers en question, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.			
4. La Commission suit, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui pourraient porter atteinte au fonctionnement des décisions adoptées en vertu du paragraphe 3.			
5. Lorsque les informations disponibles révèlent, en particulier à la suite de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 du présent article, la Commission abroge, modifie ou suspend, si nécessaire, la décision visée au paragraphe 3 du présent article par voie d'actes d'exécution sans effet rétroactif. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.			
Pour des raisons d'urgence impérieuses dûment justifiées, la Commission adopte des actes d'exécution immédiatement applicables en conformité avec la procédure visée à l'article 58, paragraphe 3.			

6. La Commission engage des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation donnant lieu à la décision adoptée en vertu du paragraphe 5.			
7 Les États membres prévoient qu'une décision adoptée en vertu du paragraphe 5 est sans préjudice des transferts de données à caractère personnel vers le pays tiers, le territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 37 et 38.			
8. La Commission publie au *Journal officiel de l'Union européenne* et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.			
Article 37 **Transferts moyennant des garanties appropriées**			
1. En l'absence de décision en vertu de l'article 36, paragraphe 3, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque:			
a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant; ou b) le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.			
2. Le responsable du traitement informe l'autorité de contrôle des catégories de transferts relevant du paragraphe 1, point b).			
3. Lorsqu'un transfert est effectué sur la base du paragraphe 1, point b), ce transfert est documenté et la documentation est mise à la disposition de l'autorité de contrôle,			

sur demande, et comporte la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, la justification du transfert et les données à caractère personnel transférées			
Article 38 **Dérogations pour des situations particulières**			
1. En l'absence de décision d'adéquation en vertu de l'article 36 ou de garanties appropriées en vertu de l'article 37, les États membres prévoient qu'un transfert ou une catégorie de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à condition que le transfert soit nécessaire:	**Article 70** Si la Commission des Communautés européennes a constaté qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données. Lorsqu'elle estime qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des Communautés européennes. Lorsqu'elle est saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et peut enjoindre au responsable du traitement de suspendre le transfert des données. Si la Commission des Communautés	Art. 70-26. - Par dérogation aux dispositions de l'article précédent, le responsable d'un traitement de données à caractère personnel ne peut, en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire :	

	européennes constate que l'Etat vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet Etat.		
a)à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne;		1° A la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne;	
b)à la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit de l'État membre transférant les données à caractère personnel le prévoit;		2° A la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit;	
c)pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers;		3° Pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre de l'Union européenne ou d'un pays tiers;	
d)dans des cas particuliers, aux fins énoncées à l'article 1er, paragraphe 1; ou		4° Dans des cas particuliers, à l'une des finalités énoncées au 1° de l'article 70-1 ;	
e)dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 1er, paragraphe 1.		5° Dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins.	
2. Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe 1, points d) et e).		Dans les cas visés aux 4° et 5°, le responsable du traitement de données à caractère personnel ne transfère pas ces données s'il estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert envisagé.	
3. Lorsqu'un transfert est effectué sur la base du paragraphe 1, point b), ce transfert est documenté et la documentation est mise à la disposition de l'autorité de contrôle,		Lorsqu'un transfert est effectué aux fins de la sauvegarde des intérêts légitimes de la personne concernée, le responsable du traitement garde trace de la date	

sur demande, et indique la date et l'heure du transfert, donne des informations sur l'autorité compétente destinataire, indique la justification du transfert et les données à caractère personnel transférées		et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et les données à caractère personnel transférées. Il met ces informations à la disposition de la Commission nationale de l'informatique et des libertés, à sa demande.	
Article 39 **Transferts de données à caractère personnel à des destinataires établis dans des pays tiers** 1. Par dérogation à l'article 35, paragraphe 1, point b), et sans préjudice de tout accord international visé au paragraphe 2 du présent article, le droit de l'Union ou le droit d'un État membre peut prévoir que les autorités compétentes au sens de l'article 3, point 7) a), peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires établis dans des pays tiers, uniquement lorsque les autres dispositions de la présente directive sont respectées et que toutes les conditions ci-après sont remplies: a)le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données ainsi que le prévoit le droit de l'Union ou le droit d'un État membre aux fins énoncées à l'article 1er, paragraphe 1; b)l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question; c)l'autorité compétente qui transfère les données estime que le transfert à une autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun; d)l'autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers		**Art. 70-27.** - Toute autorité publique compétente mentionnée au 2° de l'article 70-1 peut, dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un Etat n'appartenant pas à l'Union européenne, lorsque les autres dispositions de la présente loi applicables aux traitements relevant de l'article 70-1 sont respectées et que les conditions ci-après sont remplies : 1° Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données pour l'une des finalités énoncées à l'article 70-1 ; 2° L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas considéré ; 3° L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre État est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ; 4° L'autorité compétente de l'autre État est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ; 5° L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à	

est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié; e)l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire. 2. Par accord international visé au paragraphe 1, on entend tout accord international bilatéral ou multilatéral en vigueur entre les États membres et des pays tiers dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière. 3. L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article. 4. Lorsqu'un transfert est effectué sur la base du paragraphe 1, ce transfert est documenté.		caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire ; L'autorité compétente qui transfère des données informe la Commission nationale de l'informatique et des libertés des transferts relevant du présent article. L'autorité compétente garde trace de la date et l'heure de ce transfert, des informations sur le destinataire, et de la justification du transfert et les données à caractère personnel transférées.	
Article 40 **Coopération internationale dans le domaine de la protection des données à caractère personnel** La Commission et les États membres prennent, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour: a) élaborer des mécanismes de coopération internationaux destinés à faciliter l'application effective de la législation relative à la protection des données à caractère personnel; b) se prêter mutuellement assistance sur le plan international dans l'application de la législation relative à la protection des données à caractère personnel, notamment par la notification, la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'informations, sous réserve de garanties appropriées pour la protection des données à caractère personnel et pour d'autres libertés et droits fondamentaux;			Ces dispositions relèvent du règlement.

c) associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération internationale dans le domaine de l'application de la législation relative à la protection des données à caractère personnel; d) favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données à caractère personnel, y compris en ce qui concerne les conflits de compétence avec des pays tiers.			

CHAPITRE VI **Autorités de contrôle indépendantes** **Section 1** **Statut d'indépendance** **Article 41** **Autorité de contrôle** 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application de la présente directive, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommées «autorité de contrôle»). 2. Chaque autorité de contrôle contribue à l'application cohérente de la présente directive dans l'ensemble de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission conformément au chapitre VII. 3. Les États membres peuvent prévoir qu'une autorité de contrôle instituée au titre du règlement (UE) 2016/679 est l'autorité de contrôle visée dans la présente directive et prend en charge les missions de l'autorité de contrôle devant être instituée en vertu du paragraphe 1 du présent article. 4. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité visé à l'article 51. **Article 42** **Indépendance** 1. Chaque État membre prévoit que chaque autorité de contrôle agit en toute indépendance dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente	**Article 11 LIL** La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ; 2° Elle veille à ce que les traitements de données à caractère personnel soient mis en oeuvre conformément aux dispositions de la présente loi. A ce titre : a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ; b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ; c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ; d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en oeuvre ou envisagent de mettre en oeuvre des traitements automatisés de données à caractère personnel ; e) Elle informe sans délai le procureur de la République,		Conforme

directive. 2. Les États membres prévoient que, dans l'exercice de leurs missions et de leurs pouvoirs conformément à la présente directive, le ou les membres de leurs autorités de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque. 3. Le ou les membres des autorités de contrôle des États membres s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non. 4. Chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité. 5. Chaque État membre veille à ce que chaque autorité de contrôle choisisse et dispose de ses propres agents, qui sont placés sous les ordres exclusifs du membre ou des membres de l'autorité de contrôle concernée. 6. Chaque État membre veille à ce que chaque autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance et qu'elle dispose d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée.	conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ; f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ; g) Elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration. Il en est tenu compte, le cas échéant, pour la mise en œuvre des sanctions prévues au chapitre VII de la présente loi. h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ; 3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements : a) Elle donne un avis sur la		

	conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ; b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ; c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label . Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ; 4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des		

	droits et libertés mentionnés à l'article 1er ; A ce titre : a) Elle est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Outre les cas prévus aux articles 26 et 27, lorsqu'une loi prévoit qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté ; b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ; c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ; d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine ; e) Elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ; f) Elle promeut, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies		

	de chiffrement des données. Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi. La commission peut saisir pour avis l'Autorité de régulation des communications électroniques et des postes de toute question relevant de la compétence de celle-ci. La commission présente chaque année au Président de la République et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.		
Article 43 **Conditions générales applicables aux membres de l'autorité de contrôle** 1. Les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparente par: - leur parlement, - leur gouvernement, - leur chef d'État, ou - un organisme indépendant chargé de procéder à la nomination en vertu du droit de l'État membre. 2. Chaque membre a les qualifications, l'expérience et les compétences nécessaires, en particulier dans le domaine de la protection des données à caractère personnel, pour l'exercice de leurs fonctions et de leurs pouvoirs. 3. Les fonctions d'un membre prennent fin à l'échéance de son mandat, en cas de démission ou de mise à la retraite d'office, conformément au droit de l'État membre concerné. 4. Un membre ne peut être	**Article 13 LIL** I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres : 1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ; 2° Deux membres du Conseil économique et social, élus par cette assemblée ; 3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ; 4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ; 5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au		Conforme

démis de ses fonctions que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.	moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ; 6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ; 7° Deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat. La commission élit en son sein un président et deux vice-présidents, dont un vice-président délégué. Ils composent le bureau. La formation restreinte de la commission est composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat. En cas de partage égal des voix, celle du président est prépondérante. II. - Le mandat des membres de la commission mentionnés aux 3°, 4°, 5°, 6° et 7° du I est de cinq ans ; il est renouvelable une fois. Les membres mentionnés aux 1° et 2° siègent pour la durée du mandat à l'origine de leur désignation ; leurs mandats de membre de la Commission nationale de l'informatique et des libertés ne peuvent excéder une durée de dix ans. Le membre de la commission qui cesse d'exercer ses fonctions en cours de mandat est remplacé, dans les mêmes conditions, pour la durée de son mandat restant à courir.		

	Sauf démission, il ne peut être mis fin aux fonctions d'un membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit. La commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission.		

Article 44 **Règles relatives à l'établissement de l'autorité de contrôle** 1. Chaque État membre prévoit, par la loi, tous les éléments suivants: a) la création de chaque autorité de contrôle; b) les qualifications et les conditions d'éligibilité requises pour être nommé membre de chaque autorité de contrôle; c) les règles et les procédures pour la nomination du ou des membres de chaque autorité de contrôle; d) la durée du mandat du ou des membres de chaque autorité de contrôle, qui ne peut être inférieure à quatre ans, sauf pour la première nomination après le 6 mai 2016, dont une partie peut être d'une durée plus courte lorsque cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de nominations échelonnées; e) le caractère renouvelable ou non renouvelable du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats; f) les conditions régissant les obligations du ou des membres et des agents de chaque autorité de contrôle, les interdictions d'activités, d'emplois et d'avantages incompatibles avec celles-ci, y compris après la fin de leur mandat, et les règles régissant la cessation de l'emploi. 2. Le membre ou les membres et les agents de chaque autorité de contrôle sont soumis, conformément au droit de l'Union ou au droit de l'État membre, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans	**Article 13 LIL susvisé**		Conforme

l'exercice de leurs missions ou de leurs pouvoirs, y compris après la cessation de leurs activités. Pendant la durée de leur mandat, ce devoir de secret professionnel s'applique en particulier au signalement par des personnes physiques de violations de la présente directive.			

Article 45 **Compétence** Chaque État membre prévoit que chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément à la présente directive, sur le territoire de l'État membre dont elle relève.	**Article 5 LIL** I. - Sont soumis à la présente loi les traitements de données à caractère personnel : 1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ; 2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne. II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.		Conforme
2. Chaque État membre prévoit que chaque autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle. Les États membres peuvent prévoir que leur autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par d'autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur		**Article 4 du PJL** - L'article 44 de la même loi est ainsi modifié : 5° Il est ajouté un alinéa ainsi rédigé : *V.* - Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement	

fonction juridictionnelle.		effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions.	
Article 46 Missions 1. Chaque État membre prévoit que, sur son territoire, chaque autorité de contrôle: a) contrôle l'application des dispositions adoptées en application de la présente directive et de ses mesures d'exécution et veille au respect de celles-ci;	**Article 11 susvisé par. 2** Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.		Conforme
b) favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement;	**Article 11 par 1** La Commission : nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;		Conforme
c) conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement;	**Article 11 d)** Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ;		Conforme
d) encourage la sensibilisation des responsables du traitement et des sous-traitants aux obligations qui leur incombent en vertu de la présente directive;	**Article 11 d)** susvisé		Conforme
e) fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant de la présente directive et, le cas échéant, coopère à cette fin avec les autorités de contrôle d'autres États membres;	**Article 11 1°** Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;		Conforme

f) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association conformément à l'article 55, enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;	**Article 11 c)** Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;		Conforme. Des précisions rédactionnelles pourraient être introduites dans l'ordonnance.
g) vérifie la licéité du traitement en vertu de l'article 17, et informe la personne concernée dans un délai raisonnable de l'issue de la vérification, conformément au paragraphe 3 dudit article, ou des motifs ayant empêché sa réalisation;	**Article 11 h)** Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;		Conforme
h) coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et leur fournit une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente de la présente directive et des mesures prises pour en assurer le respect;		**Article 5 PJL** II - Après l'article 49, sont insérés les articles 49-1, 49-2, 49-3 et 49-4 ainsi rédigés : (…) **Art. 49-2**. - I- Les traitements mentionnés à l'article 70-1 font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres Etats membres de l'Union européenne dans les conditions prévues au présent article. II. - La commission communique aux autorités de contrôle des autres Etats membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que les mesures de consultation, d'inspections et d'enquête. La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après	

		réception de la demande contenant toutes les informations nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle. La Commission informe l'autorité requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre Etat membre de l'Union européenne. La commission donne les motifs de tout refus de satisfaire une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne, ou de la législation française.	
i) effectue des enquêtes sur l'application de la présente directive, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;		**Art. 49-2 susvisé**	
j) suit les évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication;	**Article 11 4**° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;		Conforme
k) fournit des conseils sur les opérations de traitement visées à l'article 28; et			Conforme

l) contribue aux activités du comité.			Le comité est institué par le règlement (UE) 2016/679 et ce règlement est directement applicable à compter de mai 2018. La définition des missions du comité (article 51 de la directive) ne relève pas de la loi française. Il pourra être précisé par décret que la CNIL « contribue » aux activités du comité.
2. Chaque autorité de contrôle facilite l'introduction des réclamations visées au paragraphe 1, point f), par des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication ne soient exclus.			Relève du décret.
3. L'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et pour le délégué à la protection des données.			Relève du décret.
4. Lorsqu'une demande est manifestement infondée ou excessive, en raison, notamment, de son caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais raisonnables basés sur ses coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle de démontrer le caractère manifestement infondé ou excessif de la demande.			Relève du décret.
Article 47 **Pouvoirs** 1. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions.	**Article 11 f)** f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;		Conforme En outre, par le maintien des formalités préalables, aucun traitement mis en œuvre pour le compte de l'Etat et relevant de la directive ne peut être mise en œuvre sans que la CNIL ait obtenu préalablement à la mise en œuvre du traitement toutes les informations nécessaires à ce traitement.

2. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices, tels que, par exemple: a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions adoptées en vertu de la présente directive; b) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions adoptées en vertu de la présente directive, le cas échéant, de manière spécifique et dans un délai déterminé, en particulier en ordonnant la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application de l'article 16; c) limiter temporairement ou définitivement, y compris interdire, un traitement.	La CNIL dispose de pouvoirs importants, notamment en application de l'article 11 4° : 4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ; A ce titre : a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés ; b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ; c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ; d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine. Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.	.	Ces pouvoirs ne sont donnés qu'à titre d'exemples («tels que, par exemple: » mentionnés dans la liste des pouvoirs. LIL déjà conforme

	La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission. **<u>Dans certains cas, la CNIL peut interdire un traitement :</u>** II. - En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire : 1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ; 2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; 3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.		
3. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs consultatifs effectifs pour conseiller le responsable du traitement conformément à la procédure de consultation			

préalable visée à l'article 28 et d'émettre, de sa propre initiative ou sur demande, des avis à l'attention de son parlement national et de son gouvernement ou, conformément à son droit national, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel.			
4. L'exercice des pouvoirs conférés à l'autorité de contrôle en application du présent article est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévues par le droit de l'Union et le droit de l'État membre conformément à la Charte.			LIL déjà conforme : toutes les décisions de la CNIL sont susceptibles de recours devant le Conseil d'Etat.
5. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle a le pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire respecter les dispositions adoptées en vertu de la présente directive. effectue des enquêtes sur l'application de la présente directive, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;	**Article 11 e) LIL** **Article 40 deuxième alinéa du code de procédure pénale** - Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.		Conforme
Article 48 **Signalement des violations** Les États membres prévoient que les autorités compétentes mettent en place des mécanismes efficaces pour encourager le signalement confidentiel des violations de la présente directive.	Législation SAPIN II en particulier articles 6, 7 et 10 de la loi SAPIN II (Loi N° LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique) **Article 6 de la loi SAPIN II** : Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral		La législation française est conforme

	d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance. Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre. **Article 7 de la loi SAPIN II** : Le chapitre II du titre II du livre Ier du code pénal est complété par un article 122-9 ainsi rédigé : Art. 122-9.-N'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte prévus à l'article 6 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. » **Article 10 de la loi SAPIN II** : I.- L'article L. 1132-3-3 du code du travail est ainsi modifié : 1° Après le premier alinéa, il est inséré un alinéa ainsi rédigé : Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation professionnelle, aucun salarié ne peut être		

	sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir signalé une alerte dans le respect des articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. » ; 2° La première phrase du second alinéa est ainsi rédigée : En cas de litige relatif à l'application des premier et deuxième alinéas, dès lors que la personne présente des éléments de fait qui permettent de présumer qu'elle a relaté ou témoigné de bonne foi de faits constitutifs d'un délit ou d'un crime, ou qu'elle a signalé une alerte dans le respect des articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 précitée, il incombe à la partie défenderesse, au vu des éléments, de prouver que sa décision est justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'intéressé. II.- L'article 6 ter A de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires est ainsi modifié : 1° Après le premier alinéa, il est inséré un alinéa ainsi rédigé : « Aucun fonctionnaire ne peut être sanctionné ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, pour avoir signalé une alerte dans le respect des		

	articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. » ; 2° La première phrase de l'avant-dernier alinéa est ainsi modifiée : a) Le mot : « trois » est remplacé par le mot : « quatre » ; b) Les mots : « ou d'une situation de conflit d'intérêts » sont remplacés par les mots : «, d'une situation de conflit d'intérêts ou d'un signalement constitutif d'une alerte au sens de l'article 6 de la loi n° 2016-1691 du 9 décembre 2016 précitée » ; 3° Le dernier alinéa est ainsi rédigé : « Le fonctionnaire qui relate ou témoigne de faits relatifs à une situation de conflit d'intérêts de mauvaise foi ou de tout fait susceptible d'entraîner des sanctions disciplinaires, avec l'intention de nuire ou avec la connaissance au moins partielle de l'inexactitude des faits rendus publics ou diffusés est puni des peines prévues au premier alinéa de l'article 226-10 du code pénal. »		
CHAPITRE VII **Coopération** **Article 50** **Assistance mutuelle** 1. Chaque État membre prévoit que leurs autorités de contrôle se communiquent les informations utiles et se prêtent mutuellement assistance en vue de mettre en œuvre et d'appliquer la présente directive de façon cohérente, et met en place des mesures pour coopérer efficacement. L'assistance mutuelle concerne notamment les demandes d'information et les mesures de contrôle, telles que les		**L'article 5 du projet de loi crée l'article 49-2 susvisé :** **Art. 49-2** I. - Les traitements mentionnés à l'article 70-1 font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres États membres de l'Union européenne dans les conditions prévues au présent article. II. - La commission communique aux autorités de contrôle des autres Etats membres les informations utiles et leur prête assistance en mettant notamment en	

demandes de consultation, les inspections et les enquêtes. 2. Chaque État membre prévoit que chaque autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande. De telles mesures peuvent comprendre notamment la transmission d'informations utiles sur la conduite d'une enquête. 3. Les demandes d'assistance contiennent toutes les informations nécessaires, notamment la finalité et les motifs de la demande. Les informations échangées ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées. 4. Une autorité de contrôle saisie d'une demande ne peut refuser d'y satisfaire, sauf si: a) elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter; ou b) satisfaire à la demande constituerait une violation de la présente directive ou du droit de l'Union ou du droit de l'État membre auquel l'autorité de contrôle qui a reçu la demande est soumise. 5. L'autorité de contrôle requise informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. L'autorité de contrôle requise donne les motifs de tout refus de satisfaire à une demande en application du paragraphe 4. 6. Les autorités de contrôle requises communiquent, en règle générale, par voie électronique et au moyen d'un formulaire type, les informations demandées par d'autres autorités de contrôle.		œuvre, à leur demande, des mesures de contrôle telles que les mesures de consultation, d'inspections et d'enquête. La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande contenant toutes les informations nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle. La Commission informe l'autorité requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre Etat membre de l'Union européenne. La commission donne les motifs de tout refus de satisfaire une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne, ou de la législation française.	

7. Les autorités de contrôle requises ne perçoivent pas de frais pour une mesure qu'elles prennent à la suite d'une demande d'assistance mutuelle. Les autorités de contrôle peuvent convenir de règles concernant l'octroi de dédommagements entre elles pour des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle dans des circonstances exceptionnelles. 8. La Commission peut, par voie d'actes d'exécution, préciser la forme et les procédures de l'assistance mutuelle visée au présent article, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.			
Article 51 **Missions du comité** 1. Le comité institué par le règlement (UE) 2016/679 exerce les missions ci-après en ce qui concerne les activités de traitement relevant du champ d'application de la présente directive: a) conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, notamment sur tout projet de modification de la présente directive; b) examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, toute question portant sur l'application de la présente directive, et publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente de la présente directive;			Ces dispositions relèvent de la Commission, et non des Etats membres

c) élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 47, paragraphes 1 et 3; d) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent alinéa, en vue d'établir les violations de données à caractère personnel et de déterminer les meilleurs délais visés à l'article 30, paragraphes 1 et 2, et de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation des données à caractère personnel; e) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent alinéa concernant les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, comme le prévoit l'article 31, paragraphe 1; f) faire le bilan de l'application pratique des lignes directrices, des recommandations et des bonnes pratiques visées aux points b) et c); g) rendre à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si ce pays tiers, ce territoire, ce secteur déterminé ou cette organisation internationale n'assure plus un niveau adéquat de protection; h) promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de bonnes			

pratiques entre les autorités de contrôle; i) promouvoir l'élaboration de programmes de formation conjoints et faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou avec des organisations internationales; j) promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur le droit et les pratiques en matière de protection des données. En ce qui concerne le point g) du premier alinéa, la Commission fournit au comité tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, le territoire ou le secteur déterminé dans ce pays tiers, ou avec l'organisation internationale. 2. Lorsque la Commission demande conseil au comité, elle peut mentionner un délai, selon l'urgence de la question. 3. Le comité transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 58, paragraphe 1, et les publie. 4. La Commission informe le comité des suites qu'elle a réservées aux avis, lignes directrices, recommandations et bonnes pratiques publiés par le comité.			
CHAPITRE VIII **Voies de recours, responsabilité et sanctions** **Article 52** **Droit d'introduire une réclamation auprès d'une autorité de contrôle** 1. Sans préjudice de tout autre recours administratif ou juridictionnel, les États			

membres prévoient que toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions adoptées en vertu de la présente directive. 2. Les États membres prévoit que, si la réclamation n'est pas introduite auprès de l'autorité de contrôle compétente au titre de l'article 45, paragraphe 1, l'autorité de contrôle auprès de laquelle la réclamation a été introduite la transmet dans les meilleurs délais à l'autorité de contrôle compétente. La personne concernée est informée de cette transmission. 3. Les États membres prévoient que l'autorité de contrôle auprès de laquelle la réclamation a été introduite fournit une assistance supplémentaire à la demande de la personne concernée. 4. La personne concernée est informée par l'autorité de contrôle compétente de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 53.			
Article 53 **Droit à un recours juridictionnel effectif contre une autorité de contrôle** 1. Sans préjudice de tout autre recours administratif ou extrajudiciaire, les États membres prévoient qu'une personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne. 2. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle qui est compétente en vertu de l'article 45, paragraphe			Ce droit existe déjà : les décisions de la CNIL sont susceptibles de recours devant le Conseil d'Etat.

1, ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 52. 3. Les États membres disposent que les actions contre une autorité de contrôle sont intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.			
Article 54 **Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant** Les États membres prévoient que, sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, notamment le droit d'introduire une réclamation auprès d'une autorité de contrôle en vertu de l'article 52, une personne concernée a droit à un recours juridictionnel effectif lorsqu'elle considère que ses droits prévus dans les dispositions adoptées en vertu de la présente directive ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation desdites dispositions.			Ce droit existe déjà et aucune disposition législative supplémentaire n'est nécessaire.
Article 55 **Représentation des personnes concernées** Les États membres prévoient, conformément à leur droit procédural, que la personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel la		**Article 16 du PJL** Après l'article 43 *ter* de la même loi, il est inséré un article 43 *quater* ainsi rédigé : **Art. 43 quater**. - La personne concernée peut mandater une association ou une organisation mentionnée au IV de l'article 43 *ter* aux fins d'exercer en son nom les droits visés aux articles 77 à 79 du règlement (UE) 2016/679. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci	

concernant, pour qu'il introduise une réclamation en son nom et exerce en son nom les droits visés aux articles 52, 53 et 54.		devant un juge ou contre le responsable du traitement ou le sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du chapitre XIII.	
Article 56 **Droit à réparation** Les États membres prévoient que toute personne ayant subi un dommage matériel ou un préjudice moral du fait d'une opération de traitement illicite ou de toute action qui constitue une violation des dispositions nationales adoptées en vertu de la présente directive a le droit d'obtenir du responsable du traitement, ou de toute autre autorité compétente en vertu du droit d'un État membre, réparation du préjudice subi.			
Article 57 **Sanctions** Les États membres déterminent le régime des sanctions applicables en cas de violations des dispositions adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives.	**L'article 45 de la LIL** prévoit des sanctions pécuniaires et des injonctions : I - Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures. Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes : 1° Un avertissement ; 2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ; 3° Une injonction de cesser le traitement, lorsque celui-		Conforme

	ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25. Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable et après une procédure contradictoire, les sanctions prévues au présent I. II. - Lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la formation restreinte, saisie par le président de la commission, peut, dans le cadre d'une procédure d'urgence définie par décret en Conseil d'Etat, après une procédure contradictoire : 1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ; 2° Prononcer un avertissement visé au 1° du I ; 3° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ; 4° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26 ; le Premier ministre fait alors connaître		

	à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue. III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés. **Par ailleurs, le code pénal incrimine diverses infractions aux articles 226-16 à 226-24 :** **Section 5 : Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.** **Article 226-16. -** Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. **Article 226-16-1-A** Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par		

	négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-16-1** Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-17** Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-17-1** Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. **Article 226-18** Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal		

	ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-18-1** Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-19** Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté. **Article 226-19-1** En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement : 1° Sans avoir préalablement		

	informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ; 2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant. **Article 226-20** Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa. **Article 226-21** Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision		

	de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-22** Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence. Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit. **Article 226-22-1** Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à		

	l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. **Article 226-22-2** Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données. **Article 226-23** Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles. **Article 226-24** Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. **<u>Enfin, toute entrave à l'action de l'autorité de contrôle est pénalement sanctionnée par l'article 51 de la LIL:</u>** **Article 51** Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés : 1° Soit en s'opposant à		

	l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ; 2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ; 3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.		
CHAPITRE IX **Actes d'exécution** **Article 58** **Comité** 1. La Commission est assistée par le comité institué par l'article 93 du règlement (UE) 2016/679. Ledit comité est un comité au sens du règlement (UE) no 182/2011. 2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique. 3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) no 182/2011 s'applique, en liaison avec son article 5.			Ne relève pas de la législation des Etats membres
CHAPITRE X **Dispositions finales** **Article 59** **Abrogation de la décision-cadre 2008/977/JAI** 1. La décision-cadre 2008/977/JAI est abrogée à compter du 6 mai 2018. 2. Les références faites à la décision abrogée visée au paragraphe 1 s'entendent comme faites à la présente directive.			Ces dispositions sont sans incidence sur la législation française

Article 60 **Actes juridiques de l'Union déjà en vigueur** Les dispositions spécifiques relatives à la protection des données à caractère personnel figurant dans des actes juridiques de l'Union qui sont entrés en vigueur le 6 mai 2016 ou avant cette date dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, qui réglementent le traitement entre États membres et l'accès des autorités nationales désignées des États membres aux systèmes d'information créés en vertu des traités, dans le cadre de la présente directive, demeurent inchangées.			Idem
Article 61 **Relation avec les accords internationaux conclus antérieurement dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière** Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant le 6 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.			Les conventions d'entraide, d'extradition et de transfèrement et les autres conventions (notamment ONU ou du Conseil de l'Europe) restent applicables jusqu'à modification de ces conventions. Des stipulations relatives à la protection des données (sur le modèle des stipulations introduites dans les conventions récentes) seront introduites progressivement.
Article 62 **Rapports de la Commission** 1. Au plus tard le 6 mai 2022, et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen de la présente directive. Ces rapports sont publiés. 2. Dans le cadre de ces évaluations et réexamens visés au paragraphe 1, la Commission examine, en particulier, l'application et le			Ne concerne pas la législation française

fonctionnement du chapitre V sur le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, en accordant une attention particulière aux décisions adoptées en vertu de l'article 36, paragraphe 3, et de l'article 39. 3. Aux fins des paragraphes 1 et 2, la Commission peut demander des informations aux États membres et aux autorités de contrôle. 4. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 et 2, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil ainsi que d'autres organismes ou sources pertinents. 5. La Commission présente, si nécessaire, des propositions législatives visant à modifier la présente directive, en particulier en tenant compte des évolutions en matière de technologie de l'information et de l'état d'avancement de la société de l'information. 6. Au plus tard le 6 mai 2019, la Commission réexamine d'autres actes juridiques adoptés par l'Union qui réglementent le traitement par les autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1, y compris ceux qui sont visés à l'article 60, afin d'apprécier la nécessité de les mettre en conformité avec la présente directive et de formuler, le cas échéant, les propositions nécessaires en vue de modifier ces actes pour assurer une approche cohérente de la protection des données à caractère personnel dans le cadre de la présente directive.			
Article 63 **Transposition** 1. Les États membres adoptent et publient, au plus tard le 6 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent		**Article 24 du PJL** Les titres I[er] à III, et les articles 21 et 22 de la présente loi entrent en vigueur à compter du 25 mai 2018. Toutefois, les dispositions de l'article 70-15 de la loi	La date d'entrée en vigueur retenue est celle du règlement. La faculté laissée par la directive d'une entrée en vigueur différée pour la journalisation est utilisée.

immédiatement à la Commission le texte de ces dispositions. Ils appliquent ces dispositions à partir du 6 mai 2018. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres. 2.Par dérogation au paragraphe 1, un État membre peut prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant le 6 mai 2016 sont mis en conformité avec l'article 25, paragraphe 1, au plus tard le 6 mai 2023. 3.Par dérogation aux paragraphes 1 et 2 du présent article, un État membre peut, dans des circonstances exceptionnelles, mettre un système donné de traitement automatisé visé au paragraphe 2 du présent article, en conformité avec l'article 25, paragraphe 1, dans un délai déterminé après le délai visé au paragraphe 2 du présent article, lorsque, à défaut de cela, de graves difficultés se poseraient pour le fonctionnement du système de traitement automatisé en question. L'État membre concerné notifie à la Commission les raisons de ces graves difficultés et les motifs justifiant le délai déterminé de mise en conformité du système donné de traitement automatisé avec l'article 25, paragraphe 1. Le délai déterminé n'est en aucun cas fixé au-delà du 6 mai 2026. 4. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.		n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans leur rédaction résultant de l'article 19 de la présente loi et relatives à l'obligation de journalisation pourront entrer en vigueur à une date ultérieure ne pouvant excéder le 6 mai 2023 lorsqu'une telle obligation exigerait des efforts disproportionnés, et ne pouvant excéder le 6 mai 2026 lorsque, à défaut d'un tel report, il en résulterait de graves difficultés pour le fonctionnement du système de traitement automatisé. La liste des traitements concernés par ces reports et les dates auxquelles, pour ces traitements, l'entrée en vigueur de cette obligation sera reportée seront déterminées par voie réglementaire.	
Article 64 Entrée en vigueur		Article 24 du PJL susvisé	

La présente directive entre en vigueur le jour suivant celui de sa publication au Journal officiel de l'Union européenne.			
Article 65 Destinataires Les États membres sont destinataires de la présente directive.			

ANNEXE 2

TABLEAU COMPARATIF - PROJET DE LOI RELATIF A LA PROTECTION DES DONNEES PERSONNELLES

Article du projet de loi	Textes existants	Modification(s)	Version consolidée
Titre I ***Dispositions communes au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016***			
Chapitre I – Dispositions relatives à la Commission nationale de l'informatique et des libertés			
Article 1er *[Dispositions relatives aux missions de la CNIL]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 11*** La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ; 2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi. A ce titre :	L'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié : 1° Au début du premier alinéa, est insérée la référence : « I. - » ; 2° Après la première phrase du premier alinéa est insérée la phrase suivante : « Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 » ; 3° Au *a* du 2° les mots : « autorise les traitements mentionnés à l'article 25, » et les mots: « et reçoit les déclarations relatives aux autres traitements » sont supprimés ;	***Article 11*** **I. -** La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. **Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679.** Elle exerce les missions suivantes : 1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ; 2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.

	a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ; b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ; c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ; d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ; e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures	4° Après le *a* du 2°, il est inséré un *a bis* ainsi rédigé : « *a bis)* Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques ; elle homologue et publie les méthodologies de référence mentionnées au IV de l'article 54, destinées à favoriser la conformité des traitement de données de santé à caractère personnel » ; 5° Le *b* du 2° est remplacé par les dispositions suivantes : « *b)* Elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données de santé relevant du chapitre IX. A ce titre, sauf pour les traitements mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures techniques et	A ce titre : a) Elle ~~**autorise les traitements mentionnés à l'article 25,**~~ donne un avis sur les traitements mentionnés aux articles 26 et 27 ~~**et reçoit les déclarations relatives aux autres traitements**~~ ; ***a bis)* Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques ; elle homologue et publie les méthodologies de référence mentionnées au IV de l'article 54, destinées à favoriser la conformité des traitement de données de santé à caractère personnel ;**

	pénales, dans les conditions prévues à l'article 52 ; f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ; g) Elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration. Il en est tenu compte, le cas échéant, pour la mise en œuvre des sanctions prévues au chapitre VII de la présente loi.	organisationnelles supplémentaires pour le traitement des données biométriques, génétiques et de santé conformément à l'article 9.4 du règlement (UE) 2016/679 et des garanties complémentaires en matière de traitement de données d'infraction conformément à l'article 10 du même règlement. » ; 6° Après le *f* du 2°, il est inséré un *f bis* ainsi rédigé : « *f bis)* Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 et la présente loi. Elle agrée, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'instance nationale d'accréditation, mentionnée à l'article 43(1) *b* du règlement, dans des conditions précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément. Elle peut établir des exigences supplémentaires aux normes d'accréditation. » ; 7° Au *g* du 2°, après le mot : « certification » sont insérés les mots : « , par des tiers agréés ou accrédités selon les modalités mentionnées au *f bis*, » ; 8° Au *h* du 2°, les mots : « d'accès concernant	**b) ~~Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;~~** ***b)* Elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données de santé relevant du chapitre IX. A ce titre, sauf pour les traitements mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures techniques et organisationnelles supplémentaires pour le traitement des données biométriques, génétiques et de santé conformément à l'article 9.4 du règlement (UE) 2016/679 et des garanties complémentaires en matière de traitement de données d'infraction conformément à l'article 10 du même règlement** ; c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

	h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ; 3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements : a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ; b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ; c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de	les traitements mentionnés aux articles 41 et 42 » sont remplacés par les mots : « d'exercice des droits prévues aux articles 41, 42 et 70-22 » ; 9° Après le *h* du 2°, il est inséré un *i* ainsi rédigé : « *i)* Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 » ; 10° Au *a* du 4°, après la première phrase, il est inséré une phrase ainsi rédigée : « Elle peut également être consultée par le président de l'Assemblée nationale ou par le président du Sénat sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données. » ; 11° Après le *f* du 4°, est inséré un alinéa ainsi rédigé : « 5° Elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement (UE) 2016/679 et de la présente loi » ; 12° Au début du vingt-sixième alinéa, est insérée la référence : « II. - ».	d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ; e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ; f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ; ***f bis*) Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 et la présente loi. Elle agrée, aux mêmes fins, des**

	l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label . Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ; 4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ; A ce titre : a) Elle est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Outre les cas prévus aux articles 26 et 27, lorsqu'une loi prévoit		**organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'instance nationale d'accréditation, mentionnée à l'article 43(1) *b* du règlement, dans des conditions précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément. Elle peut établir des exigences supplémentaires aux normes d'accréditation ;** g) Elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification**, par des tiers agréés ou accrédités selon les modalités mentionnées au f bis,** de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration. Il en est tenu compte, le cas échéant, pour la mise en œuvre des sanctions prévues au chapitre VII de la présente

	qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté ; b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ; c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ; d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine ; e) Elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ;		loi. h) Elle répond aux demandes ~~**d'accès concernant les traitements mentionnés aux articles 41 et 42**~~ **d'exercice des droits prévues aux articles 41, 42 et 70-22** ; **i) Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 ;** 3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements : a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ; b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des

	f) Elle promeut, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données. Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi. La commission peut saisir pour avis l'Autorité de régulation des communications électroniques et des postes de toute question relevant de la compétence de celle-ci. La commission présente chaque année au Président de la République et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.		droits fondamentaux des personnes ; c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label . Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ; 4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;

			A ce titre : a) Elle est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. **Elle peut également être consultée par le Président de l'Assemblée nationale ou par le Président du Sénat sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données.** Outre les cas prévus aux articles 26 et 27, lorsqu'une loi prévoit qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté ; b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ; c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ; d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à

			la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine ; e) Elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ; f) Elle promeut, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données. **5° Elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement (UE) 2016/679 et de la présente loi.** **II. -** Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la

			présente loi. La commission peut saisir pour avis l'Autorité de régulation des communications électroniques et des postes de toute question relevant de la compétence de celle-ci. La commission présente chaque année au Président de la République et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.
Article 2 *[Composition de la CNIL]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 13*** I. - La Commission nationale de l'informatique et des libertés est composée de dix-huit membres : 1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste ; 2° Deux membres du Conseil économique, social et environnemental, élus par cette assemblée ; 3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade	Au 7° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, après le mot : « numérique », sont insérés les mots : « ou des questions touchant aux libertés individuelles ».	***Article 13*** I. - La Commission nationale de l'informatique et des libertés est composée de dix-huit membres : 1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste ; 2° Deux membres du Conseil économique, social et environnemental, élus par cette assemblée ; 3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par

	au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ; 4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ; 5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ; 6° Trois personnalités qualifiées pour leur connaissance du numérique ou des questions touchant aux libertés individuelles, nommées par décret ; 7° Deux personnalités qualifiées pour leur connaissance du numérique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat ; 8° Le président de la Commission d'accès aux documents administratifs, ou son représentant. Elle comprend en outre, avec voix consultative, le Défenseur des droits		l'assemblée générale du Conseil d'Etat ; 4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ; 5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ; 6° Trois personnalités qualifiées pour leur connaissance du numérique ou des questions touchant aux libertés individuelles, nommées par décret ; 7° Deux personnalités qualifiées pour leur connaissance du numérique **ou des questions touchant aux libertés individuelles**, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat ; 8° Le président de la Commission d'accès aux documents administratifs, ou son représentant. Elle comprend en outre, avec voix consultative, le Défenseur des droits ou

	ou son représentant. Les deux membres désignés ou élus par une même autorité en application des 1° à 5° sont une femme et un homme. Les trois membres mentionnés au 6° comprennent au moins une femme et un homme. Les deux membres mentionnés au 7° sont une femme et un homme. Pour l'application de cette règle, le membre succédant à une femme est un homme et celui succédant à un homme, une femme. Toutefois, le nouveau membre désigné est de même sexe que celui qu'il remplace, soit en cas de cessation du mandat avant son terme normal, soit en cas de renouvellement du mandat de l'autre membre mentionné au 7°. Selon des modalités fixées par décret en Conseil d'Etat, le collège est, à l'exception de son président, renouvelé par moitié tous les deux ans et six mois. Le président est nommé par décret du Président de la République parmi les membres pour la durée de son mandat. La commission élit en son sein deux vice-présidents, dont un vice-président		son représentant. Les deux membres désignés ou élus par une même autorité en application des 1° à 5° sont une femme et un homme. Les trois membres mentionnés au 6° comprennent au moins une femme et un homme. Les deux membres mentionnés au 7° sont une femme et un homme. Pour l'application de cette règle, le membre succédant à une femme est un homme et celui succédant à un homme, une femme. Toutefois, le nouveau membre désigné est de même sexe que celui qu'il remplace, soit en cas de cessation du mandat avant son terme normal, soit en cas de renouvellement du mandat de l'autre membre mentionné au 7°. Selon des modalités fixées par décret en Conseil d'Etat, le collège est, à l'exception de son président, renouvelé par moitié tous les deux ans et six mois. Le président est nommé par décret du Président de la République parmi les membres pour la durée de son mandat. La commission élit en son sein deux vice-présidents, dont un vice-président délégué. Le président et les vice-

	délégué. Le président et les vice-présidents composent le bureau. Le président exerce ses fonctions à temps plein. Sa fonction est incompatible avec toute détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou de l'informatique. La durée du mandat de président est de cinq ans. Le président de la commission reçoit un traitement égal à celui afférent à la seconde des deux catégories supérieures des emplois de l'Etat classés hors échelle. La formation restreinte de la commission est composée d'un président et de cinq autres membres élus par la commission en son sein. Les membres du bureau ne sont pas éligibles à la formation restreinte. En cas de partage égal des voix, celle du président est prépondérante. II. -Le mandat des membres de la commission est de cinq ans ; il est renouvelable une fois, sous réserve des		présidents composent le bureau. Le président exerce ses fonctions à temps plein. Sa fonction est incompatible avec toute détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou de l'informatique (1). La durée du mandat de président est de cinq ans (1). Le président de la commission reçoit un traitement égal à celui afférent à la seconde des deux catégories supérieures des emplois de l'Etat classés hors échelle (1). La formation restreinte de la commission est composée d'un président et de cinq autres membres élus par la commission en son sein. Les membres du bureau ne sont pas éligibles à la formation restreinte. En cas de partage égal des voix, celle du président est prépondérante. II. -Le mandat des membres de la commission est de cinq ans ; il est renouvelable une fois, sous réserve des dixième et onzième alinéas du I.

	dixième et onzième alinéas du I. Le règlement intérieur de la commission précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11.		Le règlement intérieur de la commission précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11.
Article 3 (I et II) *[Dispositions relatives au commissaire du Gouvernement]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 17*** La formation restreinte prononce les sanctions à l'encontre des responsables de traitements qui ne respectent pas les obligations découlant de la présente loi dans les conditions prévues au chapitre VII. Les membres de la formation restreinte ne peuvent participer à l'exercice des attributions de la commission mentionnées aux c, e et f du 2° de l'article 11 et à l'article 44.	I. - Au premier alinéa de l'article 17 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, après les mots : « la formation restreinte », sont ajoutés les mots : « prend les mesures et » et après les mots : « obligations découlant » sont ajoutés les mots : « du règlement (UE) 2016/679 et ». II. - Après le premier alinéa de l'article 17 de la même loi, il est inséré un alinéa ainsi rédigé : « Les membres délibèrent hors de la présence des agents de la commission, à l'exception de ceux chargés de la tenue de la séance ».	***Article 17*** La formation restreinte **prend les mesures et** prononce les sanctions à l'encontre des responsables de traitements qui ne respectent pas les obligations découlant **du règlement (UE) 2016/679 et** de la présente loi dans les conditions prévues au chapitre VII. **Les membres délibèrent hors de la présence des agents de la commission, à l'exception de ceux chargés de la tenue de la séance.** Les membres de la formation restreinte ne peuvent participer à l'exercice des attributions de la commission mentionnées aux c, e et f du 2° de l'article 11 et à l'article 44.

Article 3 (III et IV) *[Dispositions relatives au commissaire du Gouvernement]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 18*** Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission. Des commissaires adjoints peuvent être désignés dans les mêmes conditions. Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière ou en formation restreinte, ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en vertu de l'article 16 ; il est rendu destinataire de tous ses avis et décisions. Il peut, sauf en matière de sanctions, provoquer une seconde délibération, qui doit intervenir dans les dix jours de la délibération initiale.	III. - Le deuxième alinéa de l'article 18 de la même loi est remplacé par les dispositions suivantes : « Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière, ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en vertu de l'article 16. Il peut assister aux séances de la formation restreinte, sans être présent au délibéré. Il est rendu destinataire de l'ensemble des avis et décisions de la commission et de la formation restreinte ». IV. - Le troisième alinéa de l'article 18 de la même loi est remplacé par les dispositions suivantes : « Sauf en matière de mesures ou de sanctions relevant du chapitre VII, il peut provoquer une seconde délibération de la commission, qui doit intervenir dans les dix jours de la délibération initiale ».	***Article 18*** Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission. Des commissaires adjoints peuvent être désignés dans les mêmes conditions. ~~**Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière ou en formation restreinte, ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en vertu de l'article 16 ; il est rendu destinataire de tous ses avis et décisions.**~~ **Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière, ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en vertu de l'article 16. Il peut assister aux séances de la formation restreinte, sans être présent au délibéré. Il est rendu destinataire de l'ensemble des avis et décisions de la commission et de la formation restreinte.** ~~**Il peut, sauf en matière de sanctions,**~~

			~~provoquer une seconde délibération, qui doit intervenir dans les dix jours de la délibération initiale.~~ **Sauf en matière de mesures ou de sanctions relevant du chapitre VII, il peut provoquer une seconde délibération de la commission, qui doit intervenir dans les dix jours de la délibération initiale.**
Article 4 *[Contrôle de la mise en œuvre des traitements]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 44*** I.-Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé. Le procureur de la République territorialement compétent en est préalablement informé. II. - Le responsable de locaux professionnels privés est informé de son droit d'opposition à la visite.	L'article 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié : 1° Au I, les mots : « et qui sont à usage professionnel » sont supprimés ; 2° A la première phrase du II, les mots : « de locaux professionnels privés » sont remplacés par les mots : « de ces lieux, locaux, enceintes, installations ou établissements » et à la dernière phrase du même II, après le mot : « visite » est ajouté le membre de phrase suivant : « dont la finalité est l'exercice effectif des missions prévues au III » ; 3° Au III, les trois premiers alinéas sont remplacés par deux alinéas ainsi rédigés : « Pour l'exercice des missions confiées à la Commission nationale de l'informatique et des libertés par le règlement (UE) 2016/679 et par la	***Article 44*** I.-Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel **~~et qui sont à usage professionnel~~**, à l'exclusion des parties de ceux-ci affectées au domicile privé. Le procureur de la République territorialement compétent en est préalablement informé. II. - Le responsable **~~de locaux professionnels privés~~ de ces lieux, locaux, enceintes, installations ou**

	Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter, qui statue dans des conditions fixées par décret en Conseil d'Etat. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite. La visite s'effectue sous l'autorité et le contrôle du juge des libertés et de la détention qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle. L'ordonnance ayant autorisé la visite est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout	présente loi, les membres et agents mentionnés au premier alinéa du I peuvent demander communication de tous documents, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve des dispositions de l'alinéa suivant, par le secret médical. « Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. Toutefois la communication des données médicales individuelles incluses dans cette catégorie de traitement peut être faite sous l'autorité et en présence d'un médecin. » ; 4° Après le quatrième alinéa du III, il est inséré un alinéa ainsi rédigé :	**établissements** est informé de son droit d'opposition à la visite. Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter, qui statue dans des conditions fixées par décret en Conseil d'Etat. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite **dont la finalité est l'exercice effectif des missions prévues au III.** La visite s'effectue sous l'autorité et le contrôle du juge des libertés et de la détention qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle. L'ordonnance ayant autorisé la visite est exécutoire au seul vu de la minute. Elle

	moment d'une demande de suspension ou d'arrêt de cette visite. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel devant le premier président de la cour d'appel. Celui-ci connaît également des recours contre le déroulement des opérations de visite. III.-Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent. Seul un médecin peut requérir la	« Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération nécessaire à leur mission sous une identité d'emprunt. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément à l'alinéa précédent. Un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés précise les conditions dans lesquelles ils procèdent dans ces cas à leurs constatations. » ; 5° Il est ajouté un alinéa ainsi rédigé : « *V.* - Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions. »	mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel devant le premier président de la cour d'appel. Celui-ci connaît également des recours contre le déroulement des opérations de visite. III.-**~~Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.~~** **~~Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont~~**

	communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé. En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile ; ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les		~~**ceux-ci dépendent.**~~ ~~**Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé.**~~ **Pour l'exercice des missions confiées à la Commission nationale de l'informatique et des libertés par le règlement (UE) 2016/679 et par la présente loi, les membres et agents mentionnés au premier alinéa du I peuvent demander communication de tous documents, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret**

	vérifications et visites sont effectuées sur place ou sur convocation. IV.-Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.		**ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve des dispositions de l'alinéa suivant, par le secret médical.** **Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. Toutefois la communication des données médicales individuelles incluses dans cette catégorie de traitement peut être faite sous l'autorité et en présence d'un médecin.** En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile ; ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des

			systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. **Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération nécessaire à leur mission sous une identité d'emprunt. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément à l'alinéa précédent. Un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés précise les conditions dans lesquelles ils procèdent dans ces cas à leurs constatations.** Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation. IV.-Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la

			publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article. ***V*. - Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions.**
Article 5 (I) *[Coopération de la CNIL avec d'autres autorités de contrôle]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 49*** La commission peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de l'Union européenne, procéder à des vérifications dans les mêmes conditions que celles prévues à l'article 44, sauf s'il s'agit d'un traitement mentionné aux I ou II de l'article 26. Le président de la commission ou la formation restreinte peuvent, à la demande d'une autorité exerçant des	L'article 49 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est remplacé par les dispositions suivantes : « *Art. 49.* - Dans les conditions prévues aux articles 60 à 67, du règlement (UE) 2016/679, la Commission nationale de l'informatique et des libertés met en œuvre des procédures de coopération et d'assistance mutuelle avec les autorités de contrôle des autres Etats membres de l'Union européenne, et réalise avec elles des opérations conjointes. « La commission, le président, le bureau, la formation restreinte et les agents de la	***Article 49*** ~~**La commission peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de l'Union européenne, procéder à des vérifications dans les mêmes conditions que celles prévues à l'article 44, sauf s'il s'agit d'un traitement mentionné aux I ou II de l'article 26.**~~ ~~**Le président de la commission ou la formation restreinte peuvent, à la demande d'une autorité exerçant des compétences analogues aux leurs dans**~~

	compétences analogues aux leurs dans un autre Etat membre de l'Union européenne, prendre les décisions mentionnées aux articles 45 à 47 et dans les conditions prévues par ces mêmes articles, sauf s'il s'agit d'un traitement mentionné aux I ou II de l'article 26. La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans d'autres Etats membres de la Communauté européenne.	commission mettent en œuvre, chacun pour ce qui les concerne, les procédures visées à l'alinéa précédent. »	~~**un autre Etat membre de l'Union européenne, prendre les décisions mentionnées aux articles 45 à 47 et dans les conditions prévues par ces mêmes articles, sauf s'il s'agit d'un traitement mentionné aux I ou II de l'article 26.**~~ ~~**La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans d'autres Etats membres de la Communauté européenne.**~~ ***Art 49*** **- Dans les conditions prévues aux articles 60 à 67, du règlement (UE) 2016/679, la Commission nationale de l'informatique et des libertés met en œuvre des procédures de coopération et d'assistance mutuelle avec les autorités de contrôle des autres Etats membres de l'Union européenne, et réalise avec elles des opérations conjointes.** **La commission, le président, le bureau, la formation restreinte et les agents de la commission mettent en œuvre, chacun pour ce qui les concerne, les procédures visées à l'alinéa précédent.**
Article 5 (II)		II.- Après l'article 49, sont insérés les articles	***Art. 49-1.*** **- I. - La Commission**

[Coopération de la CNIL avec d'autres autorités de contrôle] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		49-1 et 49-2 ainsi rédigés : « *Art. 49-1.* - I. - La Commission nationale de l'informatique et des libertés coopère avec les autorités de contrôle des autres Etats membres de l'Union européenne en application de l'article 62 du règlement (UE) 2016/679, dans les conditions prévues au présent article. Cette coopération n'est pas applicable aux traitements qui ne relèvent pas du champ d'application du droit de l'Union européenne. « II. - Qu'elle agisse en tant qu'autorité de contrôle chef de file ou en tant qu'autorité concernée au sens des articles 4 et 56 du règlement (UE) 2016/679, la Commission nationale de l'informatique et des libertés est compétente pour traiter une réclamation ou une éventuelle violation des dispositions du même règlement affectant par ailleurs d'autres Etats membres. Le président de la commission invite les autres autorités de contrôle concernées à participer aux opérations de contrôle conjointes qu'il décide de conduire. « III. - Lorsqu'une opération de contrôle conjointe se déroule sur le territoire français, des membres ou agents habilités de la commission, agissant en tant qu'autorité de contrôle d'accueil, sont présents aux côtés des membres et agents des autres autorités de contrôle participant, le cas échéant, à l'opération. A la demande de l'autorité de contrôle de l'Etat membre, le président de la commission peut	**nationale de l'informatique et des libertés coopère avec les autorités de contrôle des autres Etats membres de l'Union européenne en application de l'article 62 du règlement (UE) 2016/679, dans les conditions prévues au présent article. Cette coopération n'est pas applicable aux traitements qui ne relèvent pas du champ d'application du droit de l'Union européenne.** **II. - Qu'elle agisse en tant qu'autorité de contrôle chef de file ou en tant qu'autorité concernée au sens des articles 4 et 56 du règlement (UE) 2016/679, la Commission nationale de l'informatique et des libertés est compétente pour traiter une réclamation ou une éventuelle violation des dispositions du même règlement affectant par ailleurs d'autres Etats membres. Le président de la commission invite les autres autorités de contrôle concernées à participer aux opérations de contrôle conjointes qu'il décide de conduire.** **III. - Lorsqu'une opération de contrôle conjointe se déroule sur le territoire français, des membres ou agents habilités de la commission, agissant en tant qu'autorité de contrôle d'accueil, sont présents aux côtés des membres et**

		habiliter, par décision particulière, ceux des membres ou agents de l'autorité de contrôle concernée qui présentent des garanties comparables à celles requises des agents de la commission, en application des dispositions de l'article 19, à exercer, sous son autorité, tout ou partie des pouvoirs de vérification et d'enquête dont disposent les membres et les agents de la commission. « IV. - Lorsque la commission est invitée à contribuer à une opération de contrôle conjointe décidée par une autre autorité compétente, le président de la commission se prononce sur le principe et les conditions de la participation, désigne les membres et agents habilités, et en informe l'autorité requérante dans les conditions prévues à l'article 62 du règlement (UE) 2016/679. « *Art. 49-2.* - I. - Les traitements mentionnés à l'article 70-1 font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres États membres de l'Union européenne dans les conditions prévues au présent article. « II. - La commission communique aux autorités de contrôle des autres Etats membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que les mesures de consultation, d'inspections et d'enquête.	**agents des autres autorités de contrôle participant, le cas échéant, à l'opération. A la demande de l'autorité de contrôle de l'Etat membre, le président de la commission peut habiliter, par décision particulière, ceux des membres ou agents de l'autorité de contrôle concernée qui présentent des garanties comparables à celles requises des agents de la commission, en application des dispositions de l'article 19, à exercer, sous son autorité, tout ou partie des pouvoirs de vérification et d'enquête dont disposent les membres et les agents de la commission.** **IV. - Lorsque la commission est invitée à contribuer à une opération de contrôle conjointe décidée par une autre autorité compétente, le président de la commission se prononce sur le principe et les conditions de la participation, désigne les membres et agents habilités, et en informe l'autorité requérante dans les conditions prévues à l'article 62 du règlement (UE) 2016/679.** ***Art. 49-2.* - I. - Les traitements mentionnés à l'article 70-1 font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les**

		« La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande contenant toutes les informations nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle. « La Commission informe l'autorité requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. « La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre Etat membre de l'Union européenne. « La commission donne les motifs de tout refus de satisfaire une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne, ou de la législation française.	**autorités de contrôle des autres États membres de l'Union européenne dans les conditions prévues au présent article.** **II. - La commission communique aux autorités de contrôle des autres Etats membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que les mesures de consultation, d'inspections et d'enquête.** **La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande contenant toutes les informations nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle.** **La Commission informe l'autorité requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour**

			donner suite à la demande. **La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre Etat membre de l'Union européenne.** **La commission donne les motifs de tout refus de satisfaire une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne, ou de la législation française.**
Article 5 (III) *[Coopération de la CNIL avec d'autres autorités de contrôle]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		III.- Après l'article 49 bis de la même loi, sont insérés les articles 49 3 et 49 4 ainsi rédigés : « *Art. 49-3.* - Lorsque la commission agit en tant qu'autorité de contrôle chef de file s'agissant d'un traitement transfrontalier au sein de l'Union européenne, elle communique le rapport du membre rapporteur, ainsi que l'ensemble des informations utiles de la procédure ayant permis d'établir le rapport, aux autres autorités de contrôle concernées sans tarder et avant l'éventuelle audition du responsable du traitement ou du sous-traitant. Les autorités concernées sont mises en mesure d'assister à l'audition par la formation restreinte du responsable de traitement ou du sous-traitant par tout moyen de retransmission approprié, ou de prendre connaissance d'un procès-verbal dressé	***Art. 49-3.* - Lorsque la commission agit en tant qu'autorité de contrôle chef de file s'agissant d'un traitement transfrontalier au sein de l'Union européenne, elle communique le rapport du membre rapporteur, ainsi que l'ensemble des informations utiles de la procédure ayant permis d'établir le rapport, aux autres autorités de contrôle concernées sans tarder et avant l'éventuelle audition du responsable du traitement ou du sous-traitant. Les autorités concernées sont mises en mesure d'assister à l'audition par la formation restreinte du responsable de traitement ou du sous-traitant par tout moyen de retransmission approprié, ou de**

		à la suite de l'audition. « Après en avoir délibéré, la formation restreinte soumet son projet de décision aux autres autorités concernées conformément à la procédure définie à l'article 60 du règlement (UE) 2016/679. A ce titre, elle se prononce sur la prise en compte des objections pertinentes et motivées émises par les autorités concernées et saisit, si elle décide d'écarter l'une des objections, le comité européen de la protection des données conformément à l'article 65 du règlement. « Les conditions d'application du présent article sont définies par un décret en Conseil d'Etat, après avis de la Commission nationale de l'informatique et des libertés. « *Art. 49-4.* - Lorsque la commission agit en tant qu'autorité concernée, au sens du règlement (UE) 2016/679, le président de la commission est saisi des projets de mesures correctrices soumis à la commission par une autre autorité chef de file. « Lorsque ces mesures sont d'objet équivalent à celles définies aux I et III de l'article 45, le président décide, le cas échéant, d'émettre une objection pertinente et motivée selon les modalités prévues à l'article 60 de ce règlement. « Lorsque ces mesures sont d'objet équivalent à celles définies au II de l'article 45 et à l'article	**prendre connaissance d'un procès-verbal dressé à la suite de l'audition.** **Après en avoir délibéré, la formation restreinte soumet son projet de décision aux autres autorités concernées conformément à la procédure définie à l'article 60 du règlement (UE) 2016/679. A ce titre, elle se prononce sur la prise en compte des objections pertinentes et motivées émises par les autorités concernées et saisit, si elle décide d'écarter l'une des objections, le comité européen de la protection des données conformément à l'article 65 du règlement.** **Les conditions d'application du présent article sont définies par un décret en Conseil d'Etat, après avis de la Commission nationale de l'informatique et des libertés.** ***Art. 49-4.* - Lorsque la commission agit en tant qu'autorité concernée, au sens du règlement (UE) 2016/679, le président de la commission est saisi des projets de mesures correctrices soumis à la commission par une autre autorité chef de file.** **Lorsque ces mesures sont d'objet équivalent à celles définies aux I et III de l'article 45, le président décide, le**

		46, le président saisit la formation restreinte. Le président de la formation restreinte ou le membre de la formation restreinte qu'il désigne peut, le cas échéant, émettre une objection pertinente et motivée selon les mêmes modalités. »	**cas échéant, d'émettre une objection pertinente et motivée selon les modalités prévues à l'article 60 de ce règlement.** **Lorsque ces mesures sont d'objet équivalent à celles définies au II de l'article 45 et à l'article 46, le président saisit la formation restreinte. Le président de la formation restreinte ou le membre de la formation restreinte qu'il désigne peut, le cas échéant, émettre une objection pertinente et motivée selon les mêmes modalités.**
Article 6 (I et II) *[Mesures correctrices]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Chapitre VII :*** Sanctions prononcées par la formation restreinte de la Commission nationale de l'informatique et des libertés. ***Article 45*** I. - Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.	I. - L'intitulé du chapitre VII de la même loi est supprimé et remplacé par l'intitulé suivant : « Mesures et sanctions prises par la formation restreinte de la Commission nationale de l'informatique et des libertés » II. - L'article 45 de la même loi est remplacé par les dispositions suivantes : « *Art. 45.* - I. - Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 ou de la présente loi.	~~**Chapitre VII : Sanctions prononcées par la formation restreinte de la Commission nationale de l'informatique et des libertés.**~~ ***Chapitre VII :*** **Mesures et sanctions prises par la formation restreinte de la Commission nationale de l'informatique et des libertés** ***Article 45*** ~~**I. - Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de**~~

	Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes : 1° Un avertissement ; 2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ; 3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25. Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable et après une procédure contradictoire, les sanctions prévues	« II. - Lorsque le responsable du traitement ou le sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : « 1° Un rappel à l'ordre ; « 2° Une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du règlement (UE) 2016/679 ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour ; « 3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du règlement (UE) 2016/679 ou de la présente loi ; « 4° Le retrait d'une certification ou l'injonction, à l'organisme concerné, de refuser ou de retirer la certification accordée ; « 5° La suspension des flux de données	~~**faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.**~~ ~~**Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure.**~~ ~~**Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :**~~ ~~**1° Un avertissement ;**~~ ~~**2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;**~~ ~~**3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.**~~ ~~**Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut**~~

	au présent I. II. - Lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la formation restreinte, saisie par le président de la commission, peut, dans le cadre d'une procédure d'urgence définie par décret en Conseil d'Etat, après une procédure contradictoire : 1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ; 2° Prononcer un avertissement visé au 1° du I ; 3° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ;	adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ; « 6° Le retrait de la décision d'approbation d'une règle d'entreprise contraignante ; « 7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux paragraphes 5 et 6 de l'article 83 du règlement (UE) 2016/679, ces plafonds sont portés respectivement à 20 millions d'euros et 4 % du chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés à l'article 83 du règlement (UE) 2016/679. « Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce. « Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine. « Le projet de mesure est le cas échéant soumis aux autres autorités concernées selon les	**~~prononcer, sans mise en demeure préalable et après une procédure contradictoire, les sanctions prévues au présent I.~~** **~~II. - Lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la formation restreinte, saisie par le président de la commission, peut, dans le cadre d'une procédure d'urgence définie par décret en Conseil d'Etat, après une procédure contradictoire :~~** **~~1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ;~~** **~~2° Prononcer un avertissement visé au 1° du I ;~~** **~~3° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés~~**

	4° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26 ; le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue. III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.	modalités définies à l'article 60 du règlement (UE) 2016/679. « III. - Lorsque le responsable d'un traitement ou le sous-traitant ne respecte pas les obligations découlant du règlement (UE) 2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également prononcer à son égard une mise en demeure, dans le délai qu'il fixe : « 1° De satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ; « 2° De mettre les opérations de traitement en conformité avec les dispositions applicables ; « 3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense et ceux mentionnées à l'article 27, de communiquer à la personne concernée une violation de données à caractère personnel ; « 4° De rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement. « Dans le cas prévu au 4°, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou le sous-traitant de notifier aux destinataires des données les mesures qu'il a prises. « Le délai de mise en conformité peut être fixé à	~~**aux I et II de l'article 26 ;**~~ ~~**4° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26 ; le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.**~~ ~~**III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.**~~ **I. - Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 ou de la présente loi.**

		vingt-quatre heures en cas d'extrême urgence. « Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure. « Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité. »	**II. - Lorsque le responsable du traitement ou le sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :** **1° Un rappel à l'ordre ;** **2° Une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du règlement (UE) 2016/679 ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour ;** **3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du règlement (UE) 2016/679 ou de la présente loi ;**

			4° Le retrait d'une certification ou l'injonction, à l'organisme concerné, de refuser ou de retirer la certification accordée ; **5° La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;** **6° Le retrait de la décision d'approbation d'une règle d'entreprise contraignante ;** **7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux paragraphes 5 et 6 de l'article 83 du règlement (UE) 2016/679, ces plafonds sont portés respectivement à 20 millions d'euros et 4 % du chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés à l'article 83 du règlement (UE) 2016/679.**

			Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce. **Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.** **Le projet de mesure est le cas échéant soumis aux autres autorités concernées selon les modalités définies à l'article 60 du règlement (UE) 2016/679.** **III. - Lorsque le responsable d'un traitement ou le sous-traitant ne respecte pas les obligations découlant du règlement (UE) 2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également prononcer à son égard une mise en demeure, dans le délai qu'il fixe :** **1° De satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;**

			2° De mettre les opérations de traitement en conformité avec les dispositions applicables ; **3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense et ceux mentionnées à l'article 27, de communiquer à la personne concernée une violation de données à caractère personnel ;** **4° De rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement.** **Dans le cas prévu au 4°, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou le sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.** **Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d'extrême urgence.** **Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.** **Le président peut demander au bureau de rendre publique la mise en**

			demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.
Article 6 (III) *[Mesures correctrices]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 46*** Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général, les agents des services. La formation restreinte peut rendre publiques les sanctions qu'elle prononce. Elle peut ordonner que les personnes sanctionnées informent	III.- L'article 46 de la même loi est remplacé par les dispositions suivantes : « *Art. 46.* - I. - Lorsque le non-respect des dispositions du règlement (UE) 2016/679 ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'Etat, adopter l'une des mesures suivantes : « 1° L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 et ceux mentionnées à l'article 27 ; « 2° La limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ;	***Article 46*** ~~**Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général, les agents des services.**~~ ~~**La formation restreinte peut rendre publiques les sanctions qu'elle prononce. Elle peut ordonner que les personnes sanctionnées informent**~~

	individuellement de cette sanction, à leur frais, chacune des personnes concernées. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Le président de la commission peut demander au bureau de rendre publique la mise en demeure prévue au deuxième alinéa du I de l'article 45. Lorsque le président de la commission prononce la clôture de la procédure dans les conditions définies au troisième alinéa du même I, la clôture fait l'objet de la même mesure de publicité que celle, le cas échéant, de la mise en demeure. Les décisions prises par la formation restreinte au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.	« 3° La suspension provisoire de la certification délivrée au responsable du traitement ou au sous-traitant ; « 4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ; « 5° La suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 54 du chapitre IX de la présente loi. « 6° L'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 ou de la présente loi, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour ; « 7° Un rappel à l'ordre ; « 8° L'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue. « II. - Dans les circonstances exceptionnelles	~~**individuellement de cette sanction, à leur frais, chacune des personnes concernées. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Le président de la commission peut demander au bureau de rendre publique la mise en demeure prévue au deuxième alinéa du I de l'article 45. Lorsque le président de la commission prononce la clôture de la procédure dans les conditions définies au troisième alinéa du même I, la clôture fait l'objet de la même mesure de publicité que celle, le cas échéant, de la mise en demeure.**~~ ~~**Les décisions prises par la formation restreinte au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.**~~ **Article 46** **I. - Lorsque le non-respect des dispositions du règlement (UE) 2016/679 ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er et que le**

		prévues au 1 de l'article 66 du règlement (UE) 2016/679, lorsque la formation restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres autorités de contrôle concernées, le Comité européen de la protection des données et la Commission européenne. « Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement. « III. - Pour les traitements régis par le chapitre XIII, lorsqu'une autorité de contrôle compétente en vertu du règlement (UE) 2016/679 n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 de ce règlement. « IV. **-** En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la	**président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'Etat, adopter l'une des mesures suivantes :** **1° L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 et ceux mentionnées à l'article 27 ;** **2° La limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ;** **3° La suspension provisoire de la certification délivrée au responsable du traitement ou au sous-traitant ;** **4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ;**

		sauvegarde de ces droits et libertés. »	**5° La suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 54 du chapitre IX de la présente loi.** **6° L'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 ou de la présente loi, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour ;** **7° Un rappel à l'ordre ;** **8° L'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.** **II. - Dans les circonstances exceptionnelles prévues au 1 de l'article 66 du règlement (UE) 2016/679, lorsque la formation**

			restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres autorités de contrôle concernées, le Comité européen de la protection des données et la Commission européenne. **Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement.** **III. - Pour les traitements régis par le chapitre XIII, lorsqu'une autorité de contrôle compétente en vertu du règlement (UE) 2016/679 n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 de ce règlement.** **IV. - En cas d'atteinte grave et**

			immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.
Article 6 (IV) *[Mesures correctrices]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 47*** Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission. Le montant de la sanction ne peut	IV.- L'article 47 de la même loi est remplacé par les dispositions suivantes : « *Art. 47.* - Les mesures prévues au II de l'article 45 et aux 1° à 6° du I de l'article 46 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement ou au sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général, les agents des services. « La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également	***Article 47*** ~~**Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission.**~~ ~~**Le montant de la sanction ne peut**~~

	excéder 3 millions d'euros. Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce. Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.	ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. « Sans préjudice des obligations d'information qui leur incombent en application de l'article 34 du règlement (UE) 2016/679, la formation restreinte peut ordonner que le responsable ou le sous-traitant concerné informe individuellement, à ses frais, chacune des personnes concernées de la violation des dispositions de la présente loi ou du règlement précité relevée ainsi que, le cas échéant, de la mesure prononcée. »	~~**excéder 3 millions d'euros.**~~ ~~**Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.**~~ ~~**Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.**~~ ***Art. 47.*** **- Les mesures prévues au II de l'article 45 et aux 1° à 6° du I de l'article 46 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement ou au sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte**

			peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général, les agents des services. **La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées.** **Sans préjudice des obligations d'information qui leur incombent en application de l'article 34 du règlement (UE) 2016/679, la formation restreinte peut ordonner que le responsable ou le sous-traitant concerné informe individuellement, à ses frais, chacune des personnes concernées de la violation des dispositions de la présente loi ou du règlement précité relevée ainsi que, le cas échéant, de la mesure prononcée.**
Article 6 (V) *[Mesures correctrices]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et	***Article 48*** Les pouvoirs prévus à l'article 44 ainsi qu'au I, au 1° du II et au III de l'article 45 peuvent être exercés à l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur	V.- L'article 48 de la même loi est remplacé par les dispositions suivantes : « *Art. 48.* - Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE)	***Article 48*** ~~**Les pouvoirs prévus à l'article 44 ainsi qu'au I, au 1° du II et au III de l'article 45 peuvent être exercés à l'égard des traitements dont les opérations sont mises en oeuvre, en**~~

aux libertés	le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre Etat membre de la Communauté européenne.	2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la Commission qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 45 à 47, le retrait de l'agrément qui leur a été délivré. »	~~**tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre Etat membre de la Communauté européenne.**~~ ***Art. 48.*** **- Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE) 2016/679 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la Commission qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 45 à 47, le retrait de l'agrément qui leur a été délivré.**
Chapitre II – Dispositions relatives à certaines catégories de données			
Article 7 [*Mise en conformité de l'article 8 de la loi 78-17 avec l'article 9 du règlement*] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique,	***Article 8*** I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-	L'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié : 1° Le I est ainsi rédigé : « *I.* - Il est interdit de traiter des données à caractère personnel, qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale	***Article 8*** I. - ~~**Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à**~~

aux fichiers et aux libertés	ci. II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ; 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ; 3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical : - pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ; - sous réserve qu'ils ne concernent que	ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant vie sexuelle ou l'orientation sexuelle d'une personne physique. » ; 2° Au 7° du II, les mots : « et dans les conditions prévues à l'article 25 de la présente loi » sont supprimés ; 3° Le 8° du II est remplacé par les dispositions suivantes : « *8*° Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX. » ; 4° Après le 8° du II, il est inséré un 9° ainsi rédigé : « *9*° Les traitements mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques nécessaires aux contrôles de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés ou aux agents. » ; 5° Au III, la première phrase est remplacée par la phrase suivante : « Ne sont également pas soumises à l'interdiction prévue au I les données à caractère personnel mentionnées au I qui sont appelées à	~~**la santé ou à la vie sexuelle de celles-ci.**~~ **Il est interdit de traiter des données à caractère personnel, qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant vie sexuelle ou l'orientation sexuelle d'une personne physique.** II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ; 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une

	les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ; - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ; 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ; 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ; 6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;	faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés. » Et la seconde phrase est supprimée ; 6° Le IV est remplacé par les dispositions suivantes : « *IV*. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26. »	incapacité juridique ou d'une impossibilité matérielle ; 3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical : - pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ; - sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ; - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ; 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ; 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ; 6° Les traitements nécessaires aux fins de

	7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ; 8° Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX. III. - Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions du chapitre IX ne sont pas applicables. IV. - De même, ne sont pas soumis à l'interdiction prévue au I les		la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ; 7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique ~~**et dans les conditions prévues à l'article 25 de la présente loi**~~ ; 8° ~~**Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX.**~~ **Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX.** ***9°*** **Les traitements mis en œuvre par les employeurs ou les administrations**

	traitements, automatisés ou non, justifiés par l'intérêt public et soit autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26, soit déclarés dans les conditions prévues au V de l'article 22.		**qui portent sur des données biométriques nécessaires aux contrôles de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés ou aux agents.** III. - ~~**Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25**~~. **Ne sont également pas soumises à l'interdiction prévue au I les données à caractère personnel mentionnées au I qui sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés.** ~~**Les dispositions du chapitre IX ne sont pas applicables.**~~ IV. - ~~**De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non,**~~

			~~**justifiés par l'intérêt public et soit autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26, soit déclarés dans les conditions prévues au V de l'article 22.**~~ **De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26.**
Titre II ***Marges de manœuvre permises par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE***			
Chapitre I – Champ d'application territorial des dispositions complétant le règlement (UE) 2016/679			
Article 8 *[Application du critère de résidence aux marges de manœuvre]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		Après l'article 5 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il est inséré un article 5-1 ainsi rédigé : « *Art. 5-1* - Les règles nationales, prises sur le fondement des dispositions du règlement (UE) 2016/679 renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement, s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France.	***Article 5-1*** **Les règles nationales, prises sur le fondement des dispositions du règlement (UE) 2016/679 renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement, s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France.** **Toutefois, lorsqu'est en cause un des traitements mentionnés au 2 de**

		« Toutefois, lorsqu'est en cause un des traitements mentionnés au 2 de l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne. »	**l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne.**
Chapitre II – Dispositions relatives à la simplification des formalités préalables à la mise en œuvre des traitements			
Article 9 (I) *[Allègement des formalités préalables]*	***Article 22*** I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés. I bis.-Par dérogation au 1° des I et II de l'article 27, font également l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont	I. - L'article 22 de la même loi est remplacé par les dispositions suivantes : « *Art. 22.* - Un décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés détermine les catégories de responsables de traitement et les finalités de ces traitements au vu desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. La mise en œuvre des traitements intervient sans préjudice des obligations qui incombent aux responsables de traitement ou aux sous-traitants en vertu de la section 3 du chapitre IV du règlement (UE) 2016/679. « Ne sont pas soumis aux dispositions du premier alinéa ceux des traitements portant sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire :	***Article 22*** ~~**I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.**~~ ~~**I bis.-Par dérogation au 1° des I et II de l'article 27, font également l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont**~~

	exclusivement des finalités de statistique publique, sont mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code statistique non signifiant, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique. L'utilisation du code statistique non signifiant n'est autorisée qu'au sein du service statistique public. L'opération cryptographique est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre : 1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation	« 1° Qui ont exclusivement des finalités de statistique publique, mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ; « 2° Qui ont exclusivement des finalités de recherche scientifique ou historique ; « 3° Qui mettent à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, mis en œuvre par l'Etat ou une personne morale de droit public ou une personne morale de droit privé gérant un service public. « Pour les traitements dont les finalités sont mentionnées aux 1° et 2°, le numéro d'inscription au répertoire national d'identification des personnes physiques fait l'objet préalablement d'une opération cryptographique lui substituant un code statistique non signifiant. Cette opération est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. Les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique ne sont pas soumis aux	~~exclusivement des finalités de statistique publique, sont mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code statistique non signifiant, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique. L'utilisation du code statistique non signifiant n'est autorisée qu'au sein du service statistique public. L'opération cryptographique est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.~~ ~~II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :~~ ~~1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de~~

	de celui-ci ou de toute personne justifiant d'un intérêt légitime ; 2° Les traitements mentionnés au 3° du II de l'article 8. III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé. La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel. Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de	dispositions du premier alinéa. « Pour les traitements dont les finalités sont mentionnées au 1°, l'utilisation du code statistique non signifiant n'est autorisée qu'au sein du service statistique public. « Pour les traitements dont les finalités sont mentionnées au 2°, l'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu, ne peuvent être assurés par la même personne ni par le responsable de traitement. « A l'exception des traitements mentionnés au second alinéa de l'article 55, le présent article n'est pas applicable aux traitements de données à caractère personnel dans le domaine de la santé qui sont régis par les dispositions du chapitre IX. »	~~celui-ci ou de toute personne justifiant d'un intérêt légitime ;~~ ~~2° Les traitements mentionnés au 3° du II de l'article 8.~~ ~~III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.~~ ~~La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.~~ ~~Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de~~

	l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés. IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31. V. - Les traitements de données de santé à caractère personnel mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste		**~~la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.~~** **~~En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.~~** **~~IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31.~~** **~~V. - Les traitements de données de santé à caractère personnel mis en œuvre par les organismes ou les services chargés d'une mission de~~**

	fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, afin de répondre, en cas de situation d'urgence, à une alerte sanitaire, au sens de l'article L. 1413-1 du code de la santé publique, sont soumis au régime de la déclaration préalable prévu au présent article. Le responsable de traitement rend compte chaque année à la Commission nationale de l'informatique et des libertés des traitements ainsi mis en œuvre. Les conditions dans lesquelles ces traitements peuvent utiliser le numéro d'inscription au répertoire national d'identification des personnes physiques sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.		~~**service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, afin de répondre, en cas de situation d'urgence, à une alerte sanitaire, au sens de l'article L. 1413-1 du code de la santé publique, sont soumis au régime de la déclaration préalable prévu au présent article. Le responsable de traitement rend compte chaque année à la Commission nationale de l'informatique et des libertés des traitements ainsi mis en œuvre.**~~ ~~**Les conditions dans lesquelles ces traitements peuvent utiliser le numéro d'inscription au répertoire national d'identification des personnes physiques sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.**~~ **- Un décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés détermine les catégories de responsables de traitement et les finalités de ces traitements au vu**

			desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. La mise en œuvre des traitements intervient sans préjudice des obligations qui incombent aux responsables de traitement ou aux sous-traitants en vertu de la section 3 du chapitre IV du règlement (UE) 2016/679. **Ne sont pas soumis aux dispositions du premier alinéa ceux des traitements portant sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire :** **1° Qui ont exclusivement des finalités de statistique publique, mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;** **2° Qui ont exclusivement des finalités de recherche scientifique ou historique ;** **3° Qui mettent à la disposition des**

			usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, mis en œuvre par l'Etat ou une personne morale de droit public ou une personne morale de droit privé gérant un service public. **Pour les traitements dont les finalités sont mentionnées aux 1° et 2°, le numéro d'inscription au répertoire national d'identification des personnes physiques fait l'objet préalablement d'une opération cryptographique lui substituant un code statistique non signifiant. Cette opération est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. Les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique ne sont pas soumis aux dispositions du premier alinéa.** **Pour les traitements dont les finalités sont mentionnées au 1°, l'utilisation du code statistique non signifiant n'est**

			autorisée qu'au sein du service statistique public. **Pour les traitements dont les finalités sont mentionnées au 2°, l'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu, ne peuvent être assurés par la même personne ni par le responsable de traitement.** **A l'exception des traitements mentionnés au second alinéa de l'article 55, le présent article n'est pas applicable aux traitements de données à caractère personnel dans le domaine de la santé qui sont régis par les dispositions du chapitre IX.**
Article 9 (II) *[Allègement des formalités préalables]*	***Article 27*** I.-Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : 1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant	L'article 27 de la même loi est ainsi modifié : 1° Au 2° du I : *a)* La référence : « 2° » est supprimée ; *b)* Après le mot : « Etat » sont insérés les mots : « , agissant dans l'exercice de ses prérogatives de puissance publique, » ; *c)* Après les mots : qui portent » sont insérés les mots : « sur des données génétiques ou » ; 2° Le 1° du I ainsi que les II, III et IV sont	***Article 27*** I.-Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : ~~**1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant**~~

	un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ; 2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. II.-Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : 1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ; 2° Sous réserve du 9° du I de l'article	abrogés.	~~un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;~~ ~~2~~° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat**, agissant dans l'exercice de ses prérogatives de puissance publique,** qui portent **sur des données génétiques ou** sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. ~~**II.-Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :**~~ ~~**1° Sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le**~~

	25, ceux des traitements mentionnés au I : -qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ; -qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ; -et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ; 3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ; 4° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de		~~numéro d'inscription à ce répertoire ;~~ ~~2° Sous réserve du 9° du I de l'article 25, ceux des traitements mentionnés au I :~~ ~~-qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;~~ ~~-qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;~~ ~~-et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;~~ ~~3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;~~ ~~4° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de~~

	l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques. III.-Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article. IV.-Le 1° des I et II du présent article n'est pas applicable : 1° Aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, qui sont soumis au chapitre IX de la présente loi ; 2° Aux traitements mis en œuvre afin de répondre à une alerte sanitaire en cas de situation d'urgence, qui sont soumis au V de l'article 22.		**~~l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.~~** **~~III.-Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.~~** **~~IV.-Le 1° des I et II du présent article n'est pas applicable :~~** **~~1° Aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, qui sont soumis au chapitre IX de la présente loi ;~~** **~~2° Aux traitements mis en œuvre afin de répondre à une alerte sanitaire en cas de situation d'urgence, qui sont soumis au V de l'article 22.~~**

Article 9 (III) *[Allègement des formalités préalables]*	***Article 24*** I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration. Ces normes précisent : 1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ; 2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ; 3° La ou les catégories de personnes concernées ; 4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;	Les articles 24 et 25 de la même loi n° 78-17 sont abrogés.	~~**Article 24**~~ ~~**I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.**~~ ~~**Ces normes précisent :**~~ ~~**1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;**~~ ~~**2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;**~~ ~~**3° La ou les catégories de personnes concernées ;**~~ ~~**4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;**~~

	5° La durée de conservation des données à caractère personnel. Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique. II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration. Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23. ***Article 25*** I. - Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont		~~**5° La durée de conservation des données à caractère personnel.**~~ ~~**Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique.**~~ ~~**II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.**~~ ~~**Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23.**~~ ~~**Article 25**~~ ~~**I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont**~~

	mentionnés aux articles 26 et 27 : 1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ; 2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ; 3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ; 4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou		**~~mentionnés aux articles 26 et 27 :~~** **~~1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;~~** **~~2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;~~** **~~3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;~~** **~~4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire~~**

	réglementaire ; 5° Les traitements automatisés ayant pour objet : - l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ; - l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ; 6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ; 7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ; 8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité		**~~;~~** **~~5° Les traitements automatisés ayant pour objet :~~** **~~- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;~~** **~~- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;~~** **~~6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;~~** **~~7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;~~** **~~8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité~~**

	des personnes ; 9° Par dérogation au 1° du I et aux 1° et 2° du II de l'article 27, les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de recherche scientifique ou historique, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code spécifique non signifiant, propre à chaque projet de recherche, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique. L'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu ne peuvent être assurés par la même personne ni par le responsable de traitement. L'opération cryptographique est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis		**~~des personnes ;~~** **~~9° Par dérogation au 1° du I et aux 1° et 2° du II de l'article 27, les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de recherche scientifique ou historique, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code spécifique non signifiant, propre à chaque projet de recherche, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique. L'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu ne peuvent être assurés par la même personne ni par le responsable de traitement. L'opération cryptographique est renouvelée à une fréquence définie par décret en Conseil d'Etat pris après avis~~**

	motivé et publié de la Commission nationale de l'informatique et des libertés. II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation. III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.		~~**motivé et publié de la Commission nationale de l'informatique et des libertés.**~~ ~~**II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.**~~ ~~**III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.**~~
Chapitre III – Obligations incombant aux responsables de traitements et sous-traitants			
Article 10 *[Dispositions*	***Article 35***	L'article 35 de la même loi est complété par l'alinéa suivant :	***Article 35***

relatives aux sous-traitants] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que	« Toutefois, dans le champ d'application du règlement (UE) 2016/679, le sous-traitant respecte les conditions prévues au chapitre IV de ce règlement. »	Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

	sur instruction du responsable du traitement.		**Toutefois, dans le champ d'application du règlement (UE) 2016/679, le sous-traitant respecte les conditions prévues au chapitre IV de ce règlement.**
Chapitre IV – Dispositions relatives à certaines catégories particulières de traitement			
Article 11 *[mise en œuvre des traitements relatifs aux infractions]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 9*** Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par : 1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ; 2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ; 3° [*Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004* ;] 4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles	L'article 9 de la même loi est ainsi modifié : 1° Au premier alinéa, les mots : « infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par : » sont remplacés par les mots : « condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que sous le contrôle de l'autorité publique ou par : » ; 2° Le 1° est complété par les mots suivants : « ainsi que les personnes morales de droit privé collaborant au service public de la justice, et appartenant à des catégories dont la liste est fixée par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission ; » 3° Le 3° est remplacé par les dispositions suivantes : « 3° Les personnes physiques ou morales, aux fins de leur permettre de préparer et le cas échant, d'exercer et de suivre une action en	***Article 9*** Les traitements de données à caractère personnel relatives ~~**aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par**~~ : **condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que sous le contrôle de l'autorité publique ou par :** 1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales **ainsi que les personnes morales de droit privé collaborant au service public de la justice, et appartenant à des catégories dont la liste est fixée par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission ;**

	assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.	justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée proportionnée à cette finalité ; la communication à un tiers n'est alors possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités ; » 4° Après le 4°, il est inséré un 5° ainsi rédigé : « *5°* Les réutilisateurs des informations publiques figurant dans les jugements et décisions mentionnés aux articles L. 10 du code de justice administrative et L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées. »	2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ; 3° ~~[*Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004* ;]~~ **Les personnes physiques ou morales, aux fins de leur permettre de préparer et le cas échant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée proportionnée à cette finalité ; la communication à un tiers n'est alors possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités ;** 4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits. ***5°* Les réutilisateurs des informations publiques figurant dans les jugements et décisions mentionnés aux articles**

			L. 10 du code de justice administrative et L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées.
Article 12 [*traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique et historique, ou à des fins statistiques*] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 36*** Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la présente loi. Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :	L'article 36 de la même loi est ainsi modifié : 1° Au premier alinéa, les mots : « historiques, statistiques ou scientifiques » sont remplacés par les mots : « archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques » ; 2° Les deuxième et cinquième alinéas sont abrogés ; 3° L'article est complété par l'alinéa suivant : « Lorsque les traitements de données à caractère personnel sont mis en œuvre par les services publics d'archives à des fins archivistiques dans l'intérêt public conformément à l'article L. 211-2 du code du patrimoine, les droits visés aux articles 15, 16, 18, 19, 20 et 21 du règlement (UE) 2016/679 ne s'appliquent pas dans la mesure où ces droits rendent impossible ou entravent sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités. Les conditions et garanties appropriées prévues à l'article 89 du règlement (UE) 2016/679 sont	***Article 36*** Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins **~~historiques, statistiques ou scientifiques~~ archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques** ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. **~~Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la présente loi.~~** Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :

	-soit avec l'accord exprès de la personne concernée ou en vertu de ses directives, formulées dans les conditions définies à l'article 40-1 ; -soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ; -soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article.	déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique. »	-soit avec l'accord exprès de la personne concernée ou en vertu de ses directives, formulées dans les conditions définies à l'article 40-1 ; ~~**-soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ;**~~ -soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article. **Lorsque les traitements de données à caractère personnel sont mis en œuvre par les services publics d'archives à des fins archivistiques dans l'intérêt public conformément à l'article L. 211-2 du code du patrimoine, les droits visés aux articles 15, 16, 18, 19, 20 et 21 du règlement (UE) 2016/679 ne s'appliquent pas dans la mesure où ces droits rendent impossible ou entravent sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités. Les conditions et garanties appropriées prévues à l'article 89 du règlement (UE) 2016/679 sont déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux**

			archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique.
Article 13 *[traitements de données à caractère personnel dans le domaine de la santé]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	**Chapitre IX : Traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.** ***Article 53*** Les traitements automatisés de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la présente loi, à l'exception des articles 23 et 24, du I de l'article 25 et des articles 26,32 et 38. Toutefois, le présent chapitre n'est pas applicable : 1° Aux traitements de données à caractère personnel ayant pour fin le suivi thérapeutique ou médical individuel des patients ; 2° Aux traitements permettant d'effectuer des études à partir des	Le chapitre IX de la même loi est ainsi rédigé : « *CHAPITRE IX* ***« TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL DANS LE DOMAINE DE LA SANTE.*** « *Section 1* ***« Dispositions générales*** « *Art. 53*. - Outre les dispositions du règlement (UE) 2016/679, les traitements contenant des données concernant la santé des personnes sont soumis aux dispositions du présent chapitre, à l'exception des catégories de traitements suivantes : « 1° Les traitements relevant des 1° à 6° du II de l'article 8 ; « 2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 6° du II de l'article 8 lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ; « 3° Les traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ;	~~**Chapitre IX : Traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.**~~ ~~**Article 53**~~ ~~**Les traitements automatisés de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la présente loi, à l'exception des articles 23 et 24, du I de l'article 25 et des articles 26,32 et 38.**~~ ~~**Toutefois, le présent chapitre n'est pas applicable :**~~ ~~**1° Aux traitements de données à caractère personnel ayant pour fin le suivi thérapeutique ou médical individuel des patients ;**~~ ~~**2° Aux traitements permettant d'effectuer des études à partir des données recueillies en application du**~~

	données recueillies en application du 1° lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ; 3° Aux traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ; 4° Aux traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ; 5° Aux traitements effectués par les agences régionales de santé, par l'Etat et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article ; 6° Aux traitements mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la	« 4° Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ; « 5° Les traitements effectués par les agences régionales de santé, par l'Etat et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article. « *Art. 54.* - I. - Les traitements relevant du présent chapitre ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent. « II. - Des référentiels et règlements types, au sens des *a* bis et *b* du 2° de l'article 11, s'appliquant aux traitements relevant du présent chapitre sont établis par la Commission nationale de l'informatique et des libertés en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés. « Les traitements conformes à ces référentiels et règlements types peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la Commission nationale de l'informatique une déclaration attestant de cette conformité.	~~**1° lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;**~~ ~~**3° Aux traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ;**~~ ~~**4° Aux traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;**~~ ~~**5° Aux traitements effectués par les agences régionales de santé, par l'Etat et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article ;**~~ ~~**6° Aux traitements mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de**~~

	Commission nationale de l'informatique et des libertés, afin de répondre à une alerte sanitaire, dans les conditions prévues au V de l'article 22. ***Article 54*** I.-Les traitements de données à caractère personnel ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé sont autorisés par la Commission nationale de l'informatique et des libertés, dans le respect des principes définis par la présente loi et en fonction de l'intérêt public que la recherche, l'étude ou l'évaluation présente. II.-La Commission nationale de l'informatique et des libertés prend sa décision après avis : 1° Du comité compétent de protection des personnes mentionné à l' article L. 1123-6 du code de la santé publique , pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ; 2° Du comité d'expertise pour les	« Ces référentiels, peuvent également porter sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée. « III. - Les traitements mentionnés au premier alinéa du I qui ne sont pas conformes à un référentiel ou à un règlement type mentionné au II ne peuvent être mis en œuvre qu'après autorisation par la Commission nationale de l'informatique et des libertés. « L'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique peut se saisir ou être saisi, dans des conditions définies par décret en Conseil d'Etat, par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présente le traitement. « IV. - La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques. « V. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception	~~l'informatique et des libertés, afin de répondre à une alerte sanitaire, dans les conditions prévues au V de l'article 22.~~ ~~Article 54~~ ~~Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193~~ ~~I.-Les traitements de données à caractère personnel ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé sont autorisés par la Commission nationale de l'informatique et des libertés, dans le respect des principes définis par la présente loi et en fonction de l'intérêt public que la recherche, l'étude ou l'évaluation présente.~~ ~~II.-La Commission nationale de l'informatique et des libertés prend sa décision après avis :~~ ~~1° Du comité compétent de protection des personnes mentionné à l' article L. 1123-6 du code de la santé publique , pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ;~~

	recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent II. Le comité d'expertise est composé de personnes choisies en raison de leur compétence, dans une pluralité de disciplines. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement. Il peut prévoir l'existence de plusieurs sections au sein du comité, compétentes en fonction de la nature ou de la finalité du traitement. Le comité d'expertise est soumis à l'article L. 1451-1 du code de la santé publique. Le comité d'expertise émet, dans un délai d'un mois à compter de sa saisine, un avis sur la méthodologie retenue, sur la nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu, sur la qualité scientifique du projet. Le	de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président ou lorsque l'Institut national des données de santé est saisi en application du II du présent article. « Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée acceptée. Cette disposition n'est toutefois pas applicable si l'autorisation fait l'objet d'un avis préalable en vertu des dispositions du présent chapitre et que l'avis ou les avis rendus ne sont pas expressément favorables. « *Art. 55*. - Par dérogation à l'article 54, les traitements de données de santé à caractère personnel mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites, au sens de la section 1 du chapitre III du titre I[er] du livre IV du code de la santé publique, sont soumis aux seules dispositions de la section 3 du chapitre IV du règlement (UE) 2016/79. « Les traitements mentionnés au premier alinéa qui utilisent le numéro d'inscription des personnes au répertoire national d'identification	~~**2° Du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent II.**~~ ~~**Le comité d'expertise est composé de personnes choisies en raison de leur compétence, dans une pluralité de disciplines. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement. Il peut prévoir l'existence de plusieurs sections au sein du comité, compétentes en fonction de la nature ou de la finalité du traitement. Le comité d'expertise est soumis à l' article L. 1451-1 du code de la santé publique .**~~ ~~**Le comité d'expertise émet, dans un délai d'un mois à compter de sa saisine, un avis sur la méthodologie retenue, sur la nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu,**~~

	cas échéant, le comité recommande aux demandeurs des modifications de leur projet afin de le mettre en conformité avec les obligations prévues par la présente loi. A défaut d'avis du comité dans le délai d'un mois, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours. Dans des conditions définies par décret en Conseil d'Etat, l'Institut national des données de santé, prévu à l' article L. 1462-1 du code de la santé publique , peut être saisi par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation justifiant la demande de traitement ; il peut également évoquer le cas de sa propre initiative. Dans tous les cas, il rend un avis dans un délai d'un mois à compter de sa saisine. Les dossiers présentés dans le cadre du présent chapitre, à l'exclusion des recherches mentionnées aux 1° et 2° de l'article L. 1121-1 du code de la santé publique et de celles mentionnées au 3° du même article L. 1121-1 portant sur des produits mentionnés à l'article L. 5311-1 du	des personnes physiques sont mis en œuvre dans les conditions prévues à l'article 22. « Les dérogations régies par le premier alinéa du présent article prennent fin un an après la création du traitement s'il continue à être mis en œuvre. « *Art. 56*. - Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable d'un traitement de données autorisé en application de l'article 54 les données à caractère personnel qu'ils détiennent. « Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre. « Lorsque le résultat du traitement de données est rendu public, l'identification directe ou indirecte des personnes concernées doit être impossible. « Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.	~~sur la qualité scientifique du projet. Le cas échéant, le comité recommande aux demandeurs des modifications de leur projet afin de le mettre en conformité avec les obligations prévues par la présente loi. A défaut d'avis du comité dans le délai d'un mois, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours.~~ ~~Dans des conditions définies par décret en Conseil d'Etat, l'Institut national des données de santé, prévu à l' article L. 1462-1 du code de la santé publique , peut être saisi par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation justifiant la demande de traitement ; il peut également évoquer le cas de sa propre initiative. Dans tous les cas, il rend un avis dans un délai d'un mois à compter de sa saisine.~~ ~~Les dossiers présentés dans le cadre du présent chapitre, à l'exclusion des recherches mentionnées aux 1° et 2° de l'article L. 1121-1 du code de la santé publique et de celles mentionnées au 3° du même article L. 1121-1 portant sur des produits mentionnés à l'article L. 5311-1 du même code, sont déposés~~

	même code, sont déposés auprès d'un secrétariat unique, qui assure leur orientation vers les instances compétentes . III.-Pour chaque demande, la Commission nationale de l'informatique et des libertés vérifie les garanties présentées par le demandeur pour l'application des présentes dispositions et la conformité de sa demande à ses missions ou à son objet social. Si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que pour ces données réduites. La commission statue sur la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi. IV.-Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou	« *Art. 57.* - Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53. « Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données. « Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit. « *Art. 58.* - Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont individuellement informées conformément aux dispositions du règlement (UE) 2016/679. « Toutefois, ces informations peuvent ne pas être délivrées si la personne concernée a entendu faire usage du droit qui lui est reconnu par l'article L. 1111-2 du code de la santé d'être laissée dans l'ignorance d'un diagnostic ou d'un pronostic.	~~**auprès d'un secrétariat unique, qui assure leur orientation vers les instances compétentes .**~~ ~~**III.-Pour chaque demande, la Commission nationale de l'informatique et des libertés vérifie les garanties présentées par le demandeur pour l'application des présentes dispositions et la conformité de sa demande à ses missions ou à son objet social. Si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que pour ces données réduites.**~~ ~~**La commission statue sur la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi.**~~ ~~**IV.-Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la**~~

	d'évaluation dans le domaine de la santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés. V.-Des jeux de données agrégées ou des échantillons, issus des traitements des données de santé à caractère personnel pour des finalités et dans des conditions reconnues conformes à la présente loi par la Commission nationale de l'informatique et des libertés, peuvent faire l'objet d'une mise à disposition, dans des conditions préalablement homologuées par la commission, sans que l'autorisation prévue au I du présent article soit requise. VI.-La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.	« *Art. 59.* - Sont destinataires de l'information et exercent les droits de la personne concernée par le traitement les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future, pour les majeurs protégés dont l'état ne leur permet pas de prendre seul une décision personnelle éclairée. « Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits mentionnés au premier alinéa. « Pour ces traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès	~~**santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés.**~~ ~~**V.-Des jeux de données agrégées ou des échantillons, issus des traitements des données de santé à caractère personnel pour des finalités et dans des conditions reconnues conformes à la présente loi par la Commission nationale de l'informatique et des libertés, peuvent faire l'objet d'une mise à disposition, dans des conditions préalablement homologuées par la commission, sans que l'autorisation prévue au I du présent article soit requise.**~~ ~~**VI.-La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.**~~ ~~**Article 55**~~

	Article 55 Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé en application de l'article 53. Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre. La présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées. Les données sont reçues par le responsable désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre le traitement. Ce responsable veille à la sécurité des informations et de leur traitement,	aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information et exerce seul ses droits. « Pour ces mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits. « *Art. 60.* - Une information relative aux dispositions du présent chapitre doit notamment être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé au présent chapitre. « *Section 2*	~~**Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193**~~ ~~**Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé en application de l'article 53.**~~ ~~**Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre.**~~ ~~**La présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.**~~ ~~**Les données sont reçues par le responsable désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre le traitement. Ce**~~

	ainsi qu'au respect de la finalité de celui-ci. Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal. ***Article 56*** Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53. Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données. Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si	***« Dispositions particulières aux traitements à des fins de recherche, d'étude*** ***« ou d'évaluation dans le domaine de la santé.*** « *Art. 61.* - Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis aux dispositions de la section 1 du présent chapitre, sous réserve de celles de la présente section. « *Art. 62.* - Des méthodologies de référence sont homologuées et publiées, par la Commission nationale de l'informatique et des libertés. Elles sont établies en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés. « Lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre, sans autorisation mentionnée à l'article 54, à la condition que son responsable adresse préalablement à la Commission nationale de l'informatique une déclaration attestant de cette conformité. « *Art. 63.* - L'autorisation du traitement est accordée par la Commission nationale de l'informatique et des libertés dans les conditions définies à l'article 54 et après avis :	~~**responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci.**~~ ~~**Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.**~~ ~~**Article 56**~~ ~~**Créé par Loi n°2004-801 du 6 août 2004 - art. 9 JORF 7 août 2004**~~ ~~**Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53.**~~ ~~**Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en oeuvre du traitement de données.**~~

	l'intéressé a, de son vivant, exprimé son refus par écrit. ***Article 57*** I. - Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées : 1° De la nature des informations transmises ; 2° De la finalité du traitement de données ; 3° Des personnes physiques ou morales destinataires des données ; 4° Du droit d'accès et de rectification institué aux articles 39 et 40 ; 5° Du droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement. Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons	« 1° Du comité compétent de protection des personnes mentionné à l'article L. 1123-6 du code de la santé publique, pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ; « 2° Du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent article. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la composition de ce comité et définit ses règles de fonctionnement. Le comité d'expertise est soumis à l'article L. 1451-1 du code de la santé publique. « Les dossiers présentés dans le cadre de la présente section, à l'exclusion des recherches impliquant la personne humaine, sont déposés auprès d'un secrétariat unique assuré par l'Institut national des données de santé, qui assure leur orientation vers les instances compétentes. »	~~**Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.**~~ ~~**Article 57**~~ ~~**Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193**~~ ~~**I. - Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :**~~ ~~**1° De la nature des informations transmises ;**~~ ~~**2° De la finalité du traitement de données ;**~~ ~~**3° Des personnes physiques ou morales destinataires des données ;**~~ ~~**4° Du droit d'accès et de rectification institué aux articles 39 et 40 ;**~~ ~~**5° Du droit d'opposition institué aux**~~

	légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave. II. - Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet que la recherche, l'étude ou l'évaluation, il peut être dérogé, sous réserve du III, à l'obligation d'information définie au I : 1° Pour les traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ; 2° Lorsque l'information individuelle se heurte à la difficulté de retrouver les personnes concernées. Les demandes de dérogation à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche, d'étude ou d'évaluation sont justifiées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui		~~premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement.~~ ~~Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.~~ ~~II. - Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet que la recherche, l'étude ou l'évaluation, il peut être dérogé, sous réserve du III, à l'obligation d'information définie au I :~~ ~~1° Pour les traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ;~~ ~~2° Lorsque l'information individuelle se heurte à la difficulté de retrouver les personnes concernées.~~ ~~Les demandes de dérogation à l'obligation d'informer les personnes~~

	statue sur ce point. III. - Par dérogation au I, quand les recherches, les études ou les évaluations recourent à des données de santé à caractère personnel non directement identifiantes recueillies à titre obligatoire et destinées aux services ou aux établissements de l'Etat ou des collectivités territoriales ou aux organismes de sécurité sociale, l'information des personnes concernées quant à la réutilisation possible de ces données, à des fins de recherche, d'étude ou d'évaluation, et aux modalités d'exercice de leurs droits est assurée selon des modalités définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés. ***Article 58*** Sont destinataires de l'information et exercent les droits prévus aux articles 56 et 57 les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle. Par dérogation au premier alinéa du		**~~de l'utilisation de données les concernant à des fins de recherche, d'étude ou d'évaluation sont justifiées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point.~~** **~~III. - Par dérogation au I, quand les recherches, les études ou les évaluations recourent à des données de santé à caractère personnel non directement identifiantes recueillies à titre obligatoire et destinées aux services ou aux établissements de l'Etat ou des collectivités territoriales ou aux organismes de sécurité sociale, l'information des personnes concernées quant à la réutilisation possible de ces données, à des fins de recherche, d'étude ou d'évaluation, et aux modalités d'exercice de leurs droits est assurée selon des modalités définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.~~** **~~Article 58~~** **~~Modifié par LOI n°2016-1321 du 7~~**

	présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information préalable prévue au I de l'article 57 de la présente loi peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits d'accès, de rectification et d'opposition. Pour les mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information prévue aux		~~**octobre 2016 - art. 56**~~ ~~**Sont destinataires de l'information et exercent les droits prévus aux articles 56 et 57 les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle.**~~ ~~**Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information préalable prévue au I de l'article 57 de la présente loi peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de**~~

	articles 56 et 57 et exerce seul ses droits d'accès, de rectification et d'opposition. Pour les traitements mentionnés au deuxième alinéa du présent article, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits d'accès, de rectification et d'opposition. ***Article 59***		**~~l'autorité parentale, des droits d'accès, de rectification et d'opposition.~~** **~~Pour les mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information prévue aux articles 56 et 57 et exerce seul ses droits d'accès, de rectification et d'opposition.~~** **~~Pour les traitements mentionnés au deuxième alinéa du présent article, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement~~**

	Une information relative aux dispositions du présent chapitre doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé à l'article 53. ***Article 60*** La mise en œuvre d'un traitement de données en violation des conditions prévues par le présent chapitre entraîne le retrait temporaire ou définitif, par la Commission nationale de l'informatique et des libertés, de l'autorisation délivrée en application des dispositions de l'article 54. Il en est de même en cas de refus de se soumettre aux vérifications prévues par le f du 2° de l'article 11. ***Article 61*** La transmission vers un Etat n'appartenant pas à l'Union européenne de données à caractère personnel non codées faisant l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le		**~~des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits d'accès, de rectification et d'opposition.~~** **~~Article 59~~** **~~Créé par Loi n°2004-801 du 6 août 2004 - art. 9 JORF 7 août 2004~~** **~~Une information relative aux dispositions du présent chapitre doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé à l'article 53.~~** **~~Article 60~~** **~~Créé par Loi n°2004-801 du 6 août 2004 - art. 9 JORF 7 août 2004~~** **~~La mise en oeuvre d'un traitement de données en violation des conditions prévues par le présent chapitre entraîne le retrait temporaire ou définitif, par la Commission nationale~~**

	domaine de la santé n'est autorisée, dans les conditions prévues à l'article 54, que sous réserve du respect des règles énoncées au chapitre XII.		~~**de l'informatique et des libertés, de l'autorisation délivrée en application des dispositions de l'article 54.**~~ ~~**Il en est de même en cas de refus de se soumettre aux vérifications prévues par le f du 2° de l'article 11.**~~ ~~**Article 61**~~ ~~**Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193**~~ ~~**La transmission vers un Etat n'appartenant pas à l'Union européenne de données à caractère personnel non codées faisant l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé n'est autorisée, dans les conditions prévues à l'article 54, que sous réserve du respect des règles énoncées au chapitre XII.**~~ ***CHAPITRE IX : TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL DANS LE DOMAINE DE LA SANTE.*** ***Section 1*** ***Dispositions générales*** ***Art. 53.*** **- Outre les dispositions du**

			règlement (UE) 2016/679, les traitements contenant des données concernant la santé des personnes sont soumis aux dispositions du présent chapitre, à l'exception des catégories de traitements suivantes : **1° Les traitements relevant des 1° à 6° du II de l'article 8 ;** **2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 6° du II de l'article 8 lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;** **3° Les traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ;** **4° Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;** **5° Les traitements effectués par les agences régionales de santé, par l'Etat**

			et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article. ***Art. 54.* - I. - Les traitements relevant du présent chapitre ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent.** **II. - Des référentiels et règlements types, au sens des *a* bis et *b* du 2° de l'article 11, s'appliquant aux traitements relevant du présent chapitre sont établis par la Commission nationale de l'informatique et des libertés en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.** **Les traitements conformes à ces référentiels et règlements types peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la Commission nationale de l'informatique une déclaration attestant de cette conformité.**

			Ces référentiels, peuvent également porter sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée. **III. - Les traitements mentionnés au premier alinéa du I qui ne sont pas conformes à un référentiel ou à un règlement type mentionné au II ne peuvent être mis en œuvre qu'après autorisation par la Commission nationale de l'informatique et des libertés.** **L'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique peut se saisir ou être saisi, dans des conditions définies par décret en Conseil d'Etat, par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présente le traitement.** **IV. - La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de**

			données identiques et ayant des catégories de destinataires identiques. **V. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président ou lorsque l'Institut national des données de santé est saisi en application du II du présent article.** **Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée acceptée. Cette disposition n'est toutefois pas applicable si l'autorisation fait l'objet d'un avis préalable en vertu des dispositions du présent chapitre et que l'avis ou les avis rendus ne sont pas expressément favorables.** ***Art. 55.* - Par dérogation à l'article 54, les traitements de données de santé à caractère personnel mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, ayant pour seule finalité de répondre, en cas**

			de situation d'urgence, à une alerte sanitaire et d'en gérer les suites, au sens de la section 1 du chapitre III du titre I[er] du livre IV du code de la santé publique, sont soumis aux seules dispositions de la section 3 du chapitre IV du règlement (UE) 2016/79. **Les traitements mentionnés au premier alinéa qui utilisent le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques sont mis en œuvre dans les conditions prévues à l'article 22.** **Les dérogations régies par le premier alinéa du présent article prennent fin un an après la création du traitement s'il continue à être mis en œuvre.** ***Art. 56.*** **- Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable d'un traitement de données autorisé en application de l'article 54 les données à caractère personnel qu'ils détiennent.** **Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des**

			libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre. **Lorsque le résultat du traitement de données est rendu public, l'identification directe ou indirecte des personnes concernées doit être impossible.** **Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.** ***Art. 57.*** **- Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53.** **Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données.**

			Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit. ***Art. 58.*** **- Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont individuellement informées conformément aux dispositions du règlement (UE) 2016/679.** **Toutefois, ces informations peuvent ne pas être délivrées si la personne concernée a entendu faire usage du droit qui lui est reconnu par l'article L. 1111-2 du code de la santé d'être laissée dans l'ignorance d'un diagnostic ou d'un pronostic.** ***Art. 59.*** **- Sont destinataires de l'information et exercent les droits de la personne concernée par le traitement les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future,**

			pour les majeurs protégés dont l'état ne leur permet pas de prendre seul une décision personnelle éclairée. **Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits mentionnés au premier alinéa.** **Pour ces traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de**

			l'évaluation. Le mineur reçoit alors l'information et exerce seul ses droits. **Pour ces mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits.** ***Art. 60.*** **- Une information relative aux dispositions du présent chapitre doit notamment être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la**

			transmission de données à caractère personnel en vue d'un traitement visé au présent chapitre. ***Section 2*** ***Dispositions particulières aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.*** ***Art. 61.*** **- Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis aux dispositions de la section 1 du présent chapitre, sous réserve de celles de la présente section.** ***Art. 62.*** **- Des méthodologies de référence sont homologuées et publiées, par la Commission nationale de l'informatique et des libertés. Elles sont établies en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.** **Lorsque le traitement est conforme à une méthodologie de référence, il peut**

			être mis en œuvre, sans autorisation mentionnée à l'article 54, à la condition que son responsable adresse préalablement à la Commission nationale de l'informatique une déclaration attestant de cette conformité. ***Art. 63.*** **- L'autorisation du traitement est accordée par la Commission nationale de l'informatique et des libertés dans les conditions définies à l'article 54 et après avis :** **1° Du comité compétent de protection des personnes mentionné à l'article L. 1123-6 du code de la santé publique, pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ;** **2° Du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent article. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la composition de ce comité et définit ses**

			règles de fonctionnement. Le comité d'expertise est soumis à l'article L. 1451-1 du code de la santé publique. **Les dossiers présentés dans le cadre de la présente section, à l'exclusion des recherches impliquant la personne humaine, sont déposés auprès d'un secrétariat unique assuré par l'Institut national des données de santé, qui assure leur orientation vers les instances compétentes.**
Chapitre IV – Dispositions particulières relatives aux droits des personnes concernées			
Article 14 *[Décision individuelle automatisée]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 10*** Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. Ne sont pas regardées comme prises	L'article 10 de la même loi est ainsi modifié : 1° Au deuxième alinéa : *a)* Les mots : « Outre les cas mentionnés aux *a* et *c* sous le 2 de l'article 22 du règlement 2016/679 » sont introduits au début de la première phrase ; *b)* Les mots : « définir le profil de l'intéressé » sont remplacés par le mot : « prévoir » ; *c)* Les mots : « de sa personnalité » sont remplacés par les mots : « personnels relatifs à la personne concernée, à l'exception des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre I^{er} du titre I^{er} du livre IV du code des relations du public et de l'administration, à condition que le traitement ne porte pas sur des	***Article 10*** Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. **Outre les cas mentionnés aux *a* et *c* sous le 2 de l'article 22 du règlement 2016/679** aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à ~~**définir le profil de l'intéressé**~~ **prévoir** ou à évaluer certains aspects ~~**de sa**~~

	sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.	données mentionnées au I de l'article 8, » ; 2° Le troisième alinéa est remplacé par les dispositions suivantes : « Pour les décisions administratives mentionnées à l'alinéa précédent, le responsable du traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions ».	**~~personnalité.~~ personnels relatifs à la personne concernée, à l'exception des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre I^er^ du titre I^er^ du livre IV du code des relations du public et de l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8.** **~~Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.~~** **Pour les décisions administratives mentionnées à l'alinéa précédent, le responsable du traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions**
Article 15 *[Age de consentement des mineurs : marge de 13 à 16 ans]*	***Article 40*** […] II. — Sur demande de la personne concernée, le responsable du	Après le II de l'article 40 de la même loi sont insérées les dispositions suivantes : « *III.* - Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste des traitements et des catégories de traitements	***Article 40*** […] II. — Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci. En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation. Les deux premiers alinéas du présent	autorisés à déroger au droit à la communication d'une violation de données régi par l'article 34 du, règlement (UE) 2016/679 lorsque la notification d'une divulgation ou d'un accès non autorisé à ces données est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique. La dérogation prévue au présent alinéa n'est applicable qu'aux seuls traitements de données à caractère personnel nécessaires au respect d'une obligation légale qui requiert le traitement de ces données ou nécessaires à l'exercice d'une mission d'intérêt public dont est investi le responsable de traitement. »	délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci. En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation. Les deux premiers alinéas du présent II ne s'appliquent pas lorsque le traitement de données à caractère personnel est

	II ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire : 1° Pour exercer le droit à la liberté d'expression et d'information ; 2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; 3° Pour des motifs d'intérêt public dans le domaine de la santé publique ; 4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ; 5° A la constatation, à l'exercice ou à la défense de droits en justice.		nécessaire : 1° Pour exercer le droit à la liberté d'expression et d'information ; 2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; 3° Pour des motifs d'intérêt public dans le domaine de la santé publique ; 4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ; 5° A la constatation, à l'exercice ou à la défense de droits en justice. ***III*. - Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste des traitements et des catégories de traitements autorisés à déroger au droit à la communication d'une**

			violation de données régi par l'article 34 du, règlement (UE) 2016/679 lorsque la notification d'une divulgation ou d'un accès non autorisé à ces données est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique. La dérogation prévue au présent alinéa n'est applicable qu'aux seuls traitements de données à caractère personnel nécessaires au respect d'une obligation légale qui requiert le traitement de ces données ou nécessaires à l'exercice d'une mission d'intérêt public dont est investi le responsable de traitement.
Chapitre V – Voies de recours			
Article 16 *[Introduction d'une action de groupe avec mandat]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		Après l'article 43 *ter* de la même loi, il est inséré un article 43 *quater* ainsi rédigé : « *Art. 43 quater*. - La personne concernée peut mandater une association ou une organisation mentionnée au IV de l'article 43 *ter* aux fins d'exercer en son nom les droits visés aux articles 77 à 79 du règlement (UE) 2016/679. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable du traitement ou le sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du chapitre XIII. »	***Art. 43 quater*. - La personne concernée peut mandater une association ou une organisation mentionnée au IV de l'article 43 *ter* aux fins d'exercer en son nom les droits visés aux articles 77 à 79 du règlement (UE) 2016/679. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable du traitement ou le sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du chapitre XIII.**

Article 17 *[Aménagement d'une voie de recours définie par l'arrêt CJUE - C-362/14 §65]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés		La section 2 du chapitre V de la même loi est complétée par un article 43 *quinquies* ainsi rédigé : « *Art. 43 quinquies*. - Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits et libertés dans le cadre de sa mission, elle peut demander au Conseil d'Etat d'ordonner la suspension ou la cessation du transfert de données en cause, le cas échéant sous astreinte, et assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 du même règlement. Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle, la Commission nationale de l'informatique et des libertés peut saisir dans les mêmes conditions le	***Art. 43 quinquies*. - Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits et libertés dans le cadre de sa mission, elle peut demander au Conseil d'Etat d'ordonner la suspension ou la cessation du transfert de données en cause, le cas échéant sous astreinte, et assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 du même règlement. Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par**

		Conseil d'Etat pour obtenir la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation. »	**une juridiction dans l'exercice de sa fonction juridictionnelle, la Commission nationale de l'informatique et des libertés peut saisir dans les mêmes conditions le Conseil d'Etat pour obtenir la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation.**
Titre III ***Dispositions portant transposition de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données***			
Article 18 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 32*** I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle	I. - A l'avant-dernier alinéa de l'article 32 de la même loi, les mots : « ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté » sont remplacés par les mots : « , sans préjudice de l'application des dispositions du chapitre XIII ». II. - Le dernier alinéa de l'article 32 est supprimé. III. - A l'article 41 de la même loi, après les mots : « sécurité publique » sont insérés les	***Article 32*** I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle de

	de son représentant ; 2° De la finalité poursuivie par le traitement auquel les données sont destinées ; 3° Du caractère obligatoire ou facultatif des réponses ; 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ; 5° Des destinataires ou catégories de destinataires des données ; 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.	mots : « , sous réserve de l'application des dispositions du chapitre XIII, ». IV. - A l'article 42 de la même loi, les mots : « prévenir, rechercher ou constater des infractions, ou de » sont supprimés.	son représentant ; 2° De la finalité poursuivie par le traitement auquel les données sont destinées ; 3° Du caractère obligatoire ou facultatif des réponses ; 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ; 5° Des destinataires ou catégories de destinataires des données ; 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci

	Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. II. - Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; - des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.		doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. II. - Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; - des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle. Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou

	Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur : - soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; - soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. III.-Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données. Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements		l'inscription d'informations dans l'équipement terminal de l'utilisateur : - soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; - soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. III.-Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données. Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les

	nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche. IV.-Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I. V.-Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues		conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche. IV.-Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I. V.-Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ~~**ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté**~~, **sans préjudice de l'application des dispositions du chapitre XIII** dans la mesure où une

	au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement. VI.-Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales. ***Article 41*** Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient. La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications		telle limitation est nécessaire au respect des fins poursuivies par le traitement. ~~**VI.-Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.**~~ ***Article 41*** Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, **sous réserve de l'application des dispositions du chapitre XIII,** le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient. La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les

	nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi. ***Article 42*** Les dispositions de l'article 41 sont applicables aux traitements mis en oeuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des		investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi. ***Article 42*** Les dispositions de l'article 41 sont applicables aux traitements mis en oeuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de ~~**prévenir, rechercher ou**~~

	infractions, ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27.		~~constater des infractions, ou de~~ contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27.
Article 19 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Chapitre XIII : Dispositions diverses.*** ***Article 71*** Des décrets en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi. L'avis rendu sur les décrets relatifs à l'application du I bis de l'article 22 et du 9° du I de l'article 25 est motivé et publié. ***Article 72*** La présente loi est applicable, dans sa rédaction résultant de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises. Par dérogation aux dispositions du cinquième alinéa du II de l'article 54, le comité d'expertise dispose d'un délai	Le chapitre XIII de la même loi devient le chapitre XIV et, après l'article 70, il est inséré les dispositions suivantes : *« CHAPITRE XIII* ***« DISPOSITIONS APPLICABLES AUX TRAITEMENTS RELEVANT DE LA DIRECTIVE (UE) 2016/680 DU 27 AVRIL 2016*** *« Section 1* ***« Dispositions générales*** « *Art. 70-1.* - Les dispositions du présent chapitre s'appliquent, le cas échéant par dérogation aux autres dispositions de la présente loi, aux traitements des données à caractère personnel mis en œuvre : « 1° A des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; « 2° Par toute autorité publique compétente pour l'une des finalités énoncées au 1°, ou tout autre organisme ou entité à qui a été confié, à ces	~~**Chapitre XIII : Dispositions diverses.**~~ ~~**Article 71**~~ ~~**Des décrets en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi. L'avis rendu sur les décrets relatifs à l'application du I bis de l'article 22 et du 9° du I de l'article 25 est motivé et publié.**~~ ~~**Article 72**~~ ~~**La présente loi est applicable, dans sa rédaction résultant de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises.**~~ ~~**Par dérogation aux dispositions du cinquième alinéa du II de l'article 54, le comité d'expertise dispose d'un délai de deux mois pour transmettre son**~~

	de deux mois pour transmettre son avis au demandeur lorsque celui-ci réside dans l'une de ces collectivités. En cas d'urgence, ce délai peut être ramené à un mois. L'article 43 ter de la présente loi est applicable dans les îles Wallis et Futuna sous réserve, au 3° du IV, de remplacer les références : " des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail " par les mots : " des articles pertinents du code du travail applicable localement ".	mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommée autorité compétente. « Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour les finalités énoncées au 1°, par une autorité compétente au sens du 2°, et où sont respectées les dispositions des articles 70-3 et 70-4. « Pour l'application du présent chapitre, lorsque les notions utilisées ne sont pas définies au chapitre premier de la présente loi, les définitions de l'article 4 du règlement (UE) 2016/679 sont applicables. « *Art. 70-2.* - Le traitement de données mentionnées au I de l'article 8 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et, soit s'il est prévu par un acte législatif ou règlementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée. « *Art. 70-3.* - Si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités prévues au 1° de l'article 70-1, il doit être prévu par un acte règlementaire pris conformément au I de l'article 26 et aux articles 28 à 31.	~~**avis au demandeur lorsque celui-ci réside dans l'une de ces collectivités. En cas d'urgence, ce délai peut être ramené à un mois.**~~ ~~**L'article 43 ter de la présente loi est applicable dans les îles Wallis et Futuna sous réserve, au 3° du IV, de remplacer les références : " des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail " par les mots : " des articles pertinents du code du travail applicable localement ".**~~ ***CHAPITRE XIII*** ***DISPOSITIONS APPLICABLES AUX TRAITEMENTS RELEVANT DE LA DIRECTIVE (UE) 2016/680 DU 27 AVRIL 2016*** ***Section 1*** ***Dispositions générales*** ***Art. 70-1.* - Les dispositions du présent chapitre s'appliquent, le cas échéant par dérogation aux autres dispositions de la présente loi, aux traitements des données à caractère personnel mis en œuvre :** **1° A des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions**

		« Si le traitement porte sur des données mentionnées au I de l'article 8, il est prévu par un acte règlementaire pris conformément au II de l'article 26. « *Art. 70-4.* - Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable du traitement effectue une analyse d'impact relative à la protection des données à caractère personnel. « Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue par l'article 30. « Dans les autres cas, le responsable du traitement ou le sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement au traitement des données à caractère personnel : « 1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; « 2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux	**pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;** **2° Par toute autorité publique compétente pour l'une des finalités énoncées au 1°, ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommée autorité compétente.** **Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour les finalités énoncées au 1°, par une autorité compétente au sens du 2°, et où sont respectées les dispositions des articles 70-3 et 70-4.** **Pour l'application du présent chapitre, lorsque les notions utilisées ne sont pas définies au chapitre premier de la présente loi, les définitions de l'article 4 du règlement (UE) 2016/679 sont applicables.** ***Art. 70-2.* - Le traitement de données mentionnées au I de l'article 8 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et,**

		mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. « *Art. 70-5.* - Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées au 1° de l'article 70-1, ne peuvent être traitées pour d'autres finalités, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires, ou par le droit de l'Union européenne. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne. « Lorsque les autorités compétentes sont chargées d'exécuter des missions autres que celles exécutées pour les finalités énoncées au 1° de l'article 70-1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne. « Si le traitement est soumis à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions	**soit s'il est prévu par un acte législatif ou règlementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.** ***Art. 70-3.*** **- Si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités prévues au 1° de l'article 70-1, il doit être prévu par un acte règlementaire pris conformément au I de l'article 26 et aux articles 28 à 31.** **Si le traitement porte sur des données mentionnées au I de l'article 8, il est prévu par un acte règlementaire pris conformément au II de l'article 26.** ***Art. 70-4.*** **- Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable du traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.** **Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission**

		et de l'obligation de les respecter. « L'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres Etats membres ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'Etat membre dont relève l'autorité compétente qui transmet les données. « *Art. 70-6.* - Les traitements effectués pour l'une des finalités énoncées au 1° de l'article 70-1 autre que celles pour lesquelles les données ont été collectées sont autorisés sous réserve du respect des principes prévus au chapitre I[er] de la présente loi et au présent chapitre. « Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 70-1. « *Art. 70-7.* - Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques sont mis en œuvre dans les conditions de l'article 36 de la présente loi. « *Art. 70-8.* - Les données à caractère personnel fondées sur des faits sont dans la mesure du possible distinguées de celles fondées sur des	**nationale de l'informatique et des libertés avec la demande d'avis prévue par l'article 30.** **Dans les autres cas, le responsable du traitement ou le sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement au traitement des données à caractère personnel :** **1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;** **2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.** ***Art. 70-5.* - Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées au 1° de l'article 70-1, ne peuvent être traitées pour d'autres finalités, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires, ou par le droit de l'Union européenne.**

		appréciations personnelles. « *Art. 70-9.* - Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. « Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée. « Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 8 est interdit. « *Art. 70-10.* - Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant que dans les conditions prévues aux paragraphes 1, 2, 9 et 10 de l'article 28 et à l'article 29 du règlement (UE) 2016/679 et au présent article. « Les sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent chapitre et	**Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne.** **Lorsque les autorités compétentes sont chargées d'exécuter des missions autres que celles exécutées pour les finalités énoncées au 1° de l'article 70-1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne.** **Si le traitement est soumis à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.** **L'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres Etats**

		garantisse la protection des droits de la personne concernée. « Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement, et qui prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement. Le contenu de ce contrat ou acte juridique est précisé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. *« Section 2* ***« Obligations incombant aux autorités compétentes et aux responsables de traitements*** « *Art. 70-11.* - Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. « Dans la mesure du possible, lors de toute	**membres ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'Etat membre dont relève l'autorité compétente qui transmet les données.** ***Art. 70-6.*** **- Les traitements effectués pour l'une des finalités énoncées au 1° de l'article 70-1 autre que celles pour lesquelles les données ont été collectées sont autorisés sous réserve du respect des principes prévus au chapitre I[er] de la présente loi et au présent chapitre.** **Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 70-1.** ***Art. 70-7.*** **- Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques sont mis en œuvre dans les conditions de l'article 36 de la présente loi.** ***Art. 70-8.*** **- Les données à caractère personnel fondées sur des faits sont**

		transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour. « S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 70-20. « *Art. 70-12.* - Le responsable du traitement établit dans la mesure du possible et le cas échéant une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que : « 1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ; « 2° Les personnes reconnues coupables d'une infraction pénale ; « 3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;	**dans la mesure du possible distinguées de celles fondées sur des appréciations personnelles.** ***Art. 70-9.* - Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.** **Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée.** **Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 8 est interdit.** ***Art. 70-10.* - Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant que dans les conditions prévues aux paragraphes 1, 2, 9 et 10 de l'article 28 et à l'article 29 du règlement (UE) 2016/679 et au**

		« 4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux 1° et 2°. « *Art. 70-13.* - I. - Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable du traitement et le sous-traitant mettent en œuvre les mesures prévues aux paragraphes 1 et 2 de l'article 24 et aux paragraphes 1 et 2 de l'article 25 du règlement (UE) 2016/679 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8. « II. - En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à : « 1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ; « 2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés	**présent article.** **Les sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent chapitre et garantisse la protection des droits de la personne concernée.** **Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement, et qui prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement. Le contenu de ce contrat ou acte juridique est précisé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.** ***Section 2*** ***Obligations incombant aux autorités compétentes et aux responsables de traitements***

		de façon non autorisée (contrôle des supports de données) ; « 3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ; « 4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ; « 5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ; « 6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ; « 7° Garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites	***Art. 70-11.*** **- Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.** **Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour.** **S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à**

		(contrôle de l'introduction) ; « 8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ; « 9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ; « 10° Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité). « *Art. 70-14.* - Le responsable du traitement et le sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux paragraphes 1 à 4 de l'article 30 du règlement (UE) 2016/679. Ce registre contient aussi la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.	**l'article 70-20.** ***Art. 70-12.*** **- Le responsable du traitement établit dans la mesure du possible et le cas échéant une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :** **1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;** **2° Les personnes reconnues coupables d'une infraction pénale ;** **3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;** **4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux 1° et**

		« *Art. 70-15.* - Le responsable du traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation, de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données. « Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et leurs destinataires. « Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales. « Ce journal est mis à la disposition de la Commission nationale de l'informatique et des libertés à sa demande. « *Art. 70-16.* **-** Les articles 31, 33 et 34 du règlement (UE) 2016/679 sont applicables aux traitements des données à caractère personnel relevant du présent chapitre. « Si la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre Etat	**2°.** ***Art. 70-13.* - I. - Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable du traitement et le sous-traitant mettent en œuvre les mesures prévues aux paragraphes 1 et 2 de l'article 24 et aux paragraphes 1 et 2 de l'article 25 du règlement (UE) 2016/679 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8.** **II. - En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à :** **1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ;** **2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ;**

		membre ou à celui-ci, le responsable du traitement notifie également la violation au responsable du traitement de l'autre Etat membre dans les meilleurs délais. « La communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, lorsque sa mise en œuvre est de nature à mettre en danger la sécurité publique, la sécurité nationale ou les droits ou libertés d'autrui ou à faire obstacle au bon déroulement des enquêtes et procédures destinées à prévenir, détecter ou poursuivre des infractions pénales ou à exécuter des sanctions pénales. « *Art. 70-17.* - I. - Sauf pour les juridictions agissant dans l'exercice de leur fonction juridictionnelle, le responsable du traitement désigne un délégué à la protection des données. « Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille. « Les dispositions des paragraphes 5 et 7 de l'article 37, des paragraphes 1 et 2 de l'article 38	**3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ;** **4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ;** **5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ;** **6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ;** **7° Garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites**

		et du paragraphe 1 de l'article 39 du règlement (UE) 2016/679, en ce qu'elles concernent le responsable du traitement, sont applicables aux traitements des données à caractère personnel relevant du présent chapitre. *« Section 3* ***« Droits de la personne concernée*** « *Art. 70-18.* - I. - Le responsable du traitement met à la disposition de la personne concernée les informations suivantes : « 1° L'identité et les coordonnées du responsable du traitement, et le cas échéant celles de son représentant ; « 2° Le cas échéant, les coordonnées du délégué à la protection des données ; « 3° Les finalités poursuivies par le traitement auquel les données sont destinées ; « 4° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ; « 5° L'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.	**dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction) ;** **8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ;** **9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ;** **10° Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).** ***Art. 70-14.* - Le responsable du traitement et le sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux paragraphes 1 à 4 de l'article 30 du règlement (UE) 2016/679. Ce registre contient aussi la description générale**

		« II. - En plus des informations visées au I, le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits : « 1° La base juridique du traitement ; « 2° La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ; « 3° Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les Etats non membres de l'Union européenne ou au sein d'organisations internationales ; « 4° Au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée. « *Art. 70-19.* - La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes : « 1° Les finalités du traitement ainsi que sa base juridique ;	**des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 8, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.** ***Art. 70-15.*** **- Le responsable du traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation, de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données.** **Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et leurs destinataires.** **Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie**

		« 2° Les catégories de données à caractère personnel concernées ; « 3° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des Etats non membres de l'Union européenne ou les organisations internationales ; « 4° Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ; « 5° L'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement de ces données ; « 6° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ; « 7° La communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source. « *Art. 70-20.* - I. - La personne concernée a le droit d'obtenir du responsable du traitement : « 1° Que soit rectifiées dans les meilleurs délais	**de l'intégrité et de la sécurité des données et à des fins de procédures pénales.** **Ce journal est mis à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.** ***Art. 70-16.* - Les articles 31, 33 et 34 du règlement (UE) 2016/679 sont applicables aux traitements des données à caractère personnel relevant du présent chapitre.** **Si la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre Etat membre ou à celui-ci, le responsable du traitement notifie également la violation au responsable du traitement de l'autre Etat membre dans les meilleurs délais.** **La communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits**

		des données à caractère personnel la concernant qui sont inexactes ; « 2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ; « 3° Que soit effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement. « II. - Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier qu'il a procédé aux opérations exigées en vertu du I. « III. - Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque : « 1° Soit l'exactitude des données à caractère personnel est contestée par la personne concernée et il ne peut être déterminé si les données sont exactes ou non ; « 2° Soit les données à caractère personnel doivent être conservées à des fins probatoires. « Lorsque le traitement est limité en vertu du 1°, le responsable du traitement informe la personne	**fondamentaux et des intérêts légitimes de la personne physique concernée, lorsque sa mise en œuvre est de nature à mettre en danger la sécurité publique, la sécurité nationale ou les droits ou libertés d'autrui ou à faire obstacle au bon déroulement des enquêtes et procédures destinées à prévenir, détecter ou poursuivre des infractions pénales ou à exécuter des sanctions pénales.** ***Art. 70-17.*** **- I. - Sauf pour les juridictions agissant dans l'exercice de leur fonction juridictionnelle, le responsable du traitement désigne un délégué à la protection des données.** **Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille.** **Les dispositions des paragraphes 5 et 7 de l'article 37, des paragraphes 1 et 2 de l'article 38 et du paragraphe 1 de l'article 39 du règlement (UE) 2016/679, en ce qu'elles concernent le responsable du traitement, sont applicables aux traitements des données à caractère personnel relevant du présent chapitre.**

		concernée avant de lever la limitation du traitement. « IV. - Le responsable du traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. « V. - Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont elles proviennent. « VI. - Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I, II et III, le responsable du traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité. « *Art. 70-21.* - I. - Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne pour : « 1° Eviter de gêner des enquêtes, des recherches ou des procédures officielles ou	***Section 3*** ***Droits de la personne concernée*** ***Art. 70-18.*** **- I. - Le responsable du traitement met à la disposition de la personne concernée les informations suivantes :** **1° L'identité et les coordonnées du responsable du traitement, et le cas échéant celles de son représentant ;** **2° Le cas échéant, les coordonnées du délégué à la protection des données ;** **3° Les finalités poursuivies par le traitement auquel les données sont destinées ;** **4° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;** **5° L'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.** **II. - En plus des informations visées au**

		judiciaires : « 2° Eviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; « 3° Protéger la sécurité publique ; « 4° Protéger la sécurité nationale ; « 5° Protéger les droits et libertés d'autrui. « Ces restrictions sont prévues par l'acte instaurant le traitement. « II. - Lorsque les conditions prévues au I sont remplies, le responsable du traitement peut : « 1° Retarder ou limiter la fourniture à la personne concernée des informations mentionnées au II de l'article 70-18, ou ne pas fournir ces informations ; « 2° Limiter, entièrement ou partiellement, le droit d'accès de la personne concernée prévu par l'article 70-19 ; « 3° Ne pas informer la personne de son refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de cette décision conformément au IV de l'article 70-20.	**I, le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits :** **1° La base juridique du traitement ;** **2° La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;** **3° Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les Etats non membres de l'Union européenne ou au sein d'organisations internationales ;** **4° Au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.** ***Art. 70-19.* - La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations**

		« III. - Dans les cas visés au 2° du II, le responsable du traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision, et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés. « IV. - En cas de restriction des droits de la personne concernée intervenue en application du II ou du III, le responsable du traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel. « *Art. 70-22.* - En cas de restriction des droits de la personne concernée intervenue en application du II ou du III de l'article 70-21, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés. « Les dispositions des deuxième et troisième alinéas de l'article 41 sont alors applicables. « Lorsque la commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires, elle l'informe également de son	**suivantes :** **1° Les finalités du traitement ainsi que sa base juridique ;** **2° Les catégories de données à caractère personnel concernées ;** **3° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des Etats non membres de l'Union européenne ou les organisations internationales ;** **4° Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;** **5° L'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement de ces données ;** **6° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des**

		droit de former un recours juridictionnel. « *Art. 70-23.* - Aucun paiement n'est exigé pour prendre les mesures et fournir les informations visées aux articles 70-18 à 70-20, sauf en cas de demande manifestement infondée ou abusive. « Dans ce cas, le responsable du traitement peut également refuser de donner suite à la demande. « En cas de contestation, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombe au responsable du traitement auprès duquel elles sont adressées. « *Art 70-24.* - Les dispositions de la présente sous-section ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données ne peut se faire que dans les conditions prévues par le code de procédure pénale. *« Section 4* ***« Transferts de données à caractère personnel vers des Etats n'appartenant pas « à l'Union européenne ou vers des destinataires établis dans des Etats non membres « de l'Union européenne*** « *Art. 70-25.* - Le responsable d'un traitement de	**libertés et les coordonnées de la commission ;** **7° La communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.** ***Art. 70-20.* - I. - La personne concernée a le droit d'obtenir du responsable du traitement :** **1° Que soit rectifiées dans les meilleurs délais des données à caractère personnel la concernant qui sont inexactes ;** **2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ;** **3° Que soit effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.** **II. - Lorsque l'intéressé en fait la**

		données à caractère personnel ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées : « 1° Le transfert de ces données est nécessaire à l'une des finalités énoncées au 1° de l'article 70-1 ; « 2° Les données à caractère personnel sont transférées à un responsable dans cet Etat tiers ou à une organisation internationale qui est une autorité compétente chargée dans cet Etat des fins relevant en France du 1° de l'article 70-1 ; « 3° Si les données à caractère personnel proviennent d'un autre Etat, l'Etat qui a transmis ces données a préalablement autorisé ce transfert conformément à son droit national. « Toutefois, si l'autorisation préalable ne peut pas être obtenue en temps utile, ces données à caractère personnel peuvent être retransmises sans l'autorisation préalable de l'Etat qui a transmis ces données lorsque cette retransmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre Etat ou pour la sauvegarde des intérêts essentiels de la France. L'autorité d'où provenaient ces données personnelles est informée sans retard. « 4° L'une au moins des trois conditions	**demande, le responsable du traitement doit justifier qu'il a procédé aux opérations exigées en vertu du I.** **III. - Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque :** **1° Soit l'exactitude des données à caractère personnel est contestée par la personne concernée et il ne peut être déterminé si les données sont exactes ou non ;** **2° Soit les données à caractère personnel doivent être conservées à des fins probatoires.** **Lorsque le traitement est limité en vertu du 1°, le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.** **IV. - Le responsable du traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus.** **V. - Le responsable du traitement communique la rectification des données à caractère personnel**

		suivantes est remplie : « *a)* La commission a adopté une décision d'adéquation en application de l'article 36 de la directive (UE) 2016/680 du Parlement et du Conseil du 27 avril 2016 ; « *b)* A défaut d'une telle décision d'adéquation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ; ces garanties appropriées peuvent soit résulter des garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet Etat tiers, soit résulter de dispositions juridiquement contraignantes exigées à l'occasion de l'échange de données ; « *c)* A défaut d'une telle décision d'adéquation et de garanties appropriées telles que prévues au *b*, le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel ; « Lorsque le responsable d'un traitement de données à caractère personnel transfère des données à caractère personnel sur le seul fondement de l'existence de garanties appropriées au regard de la protection des données à caractère personnel, autre qu'une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles, il	**inexactes à l'autorité compétente dont elles proviennent.** **VI. - Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I, II et III, le responsable du traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.** ***Art. 70-21.* - I. - Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne pour :** **1° Eviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires :** **2° Eviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;**

		avise la Commission nationale de l'informatique et des libertés des catégories de transferts relevant de ce fondement. « Dans ce cas, le responsable du traitement des données doit garder trace de la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et des données à caractère personnel transférées. Cette documentation est mise à la disposition de l'autorité de contrôle, sur sa demande. « Lorsque la commission a abrogé, modifié ou suspendu une décision d'adéquation adoptée en application de l'article 36 de la directive précitée, le responsable d'un traitement de données à caractère personnel peut néanmoins transférer des données personnelles ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ou s'il estime après avoir évalué toutes les circonstances du transfert qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel. « *Art. 70-26.* - Par dérogation aux dispositions de l'article précédent, le responsable d'un traitement de données à caractère personnel ne peut, en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données	**3° Protéger la sécurité publique ;** **4° Protéger la sécurité nationale ;** **5° Protéger les droits et libertés d'autrui.** **Ces restrictions sont prévues par l'acte instaurant le traitement.** **II. - Lorsque les conditions prévues au I sont remplies, le responsable du traitement peut :** **1° Retarder ou limiter la fourniture à la personne concernée des informations mentionnées au II de l'article 70-18, ou ne pas fournir ces informations ;** **2° Limiter, entièrement ou partiellement, le droit d'accès de la personne concernée prévu par l'article 70-19 ;** **3° Ne pas informer la personne de son refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de cette décision conformément au IV de l'article 70-20.** **III. - Dans les cas visés au 2° du II, le responsable du traitement informe la**

		ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire : « 1° A la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ; « 2° A la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit ; « 3° Pour prévenir une menace grave et immédiate pour la sécurité publique d'un Etat membre de l'Union européenne ou d'un pays tiers ; « 4° Dans des cas particuliers, à l'une des finalités énoncées au 1° de l'article 70-1 ; « 5° Dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins. « Dans les cas visés aux 4° et 5°, le responsable du traitement de données à caractère personnel ne transfère pas ces données s'il estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert envisagé. « Lorsqu'un transfert est effectué aux fins de la sauvegarde des intérêts légitimes de la personne concernée, le responsable du traitement garde	**personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision, et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés.** **IV. - En cas de restriction des droits de la personne concernée intervenue en application du II ou du III, le responsable du traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel.** ***Art. 70-22.*** **- En cas de restriction des droits de la personne concernée intervenue en application du II ou du III de l'article 70-21, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés.** **Les dispositions des deuxième et**

		trace de la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et les données à caractère personnel transférées. Il met ces informations à la disposition de la Commission nationale de l'informatique et des libertés, à sa demande. « *Art. 70-27.* - Toute autorité publique compétente mentionnée au 2° de l'article 70-1 peut, dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un Etat n'appartenant pas à l'Union européenne, lorsque les autres dispositions de la présente loi applicables aux traitements relevant de l'article 70-1 sont respectées et que les conditions ci-après sont remplies : « 1° Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données pour l'une des finalités énoncées à l'article 70-1 ; « 2° L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas considéré ; « 3° L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre Etat est inefficace ou inapproprié, notamment parce que le transfert ne	**troisième alinéas de l'article 41 sont alors applicables.** **Lorsque la commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires, elle l'informe également de son droit de former un recours juridictionnel.** ***Art. 70-23.* - Aucun paiement n'est exigé pour prendre les mesures et fournir les informations visées aux articles 70-18 à 70-20, sauf en cas de demande manifestement infondée ou abusive.** **Dans ce cas, le responsable du traitement peut également refuser de donner suite à la demande.** **En cas de contestation, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombe au responsable du traitement auprès duquel elles sont adressées.** ***Art 70-24.* - Les dispositions de la présente sous-section ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces**

		peut pas être effectué en temps opportun ; « 4° L'autorité compétente de l'autre Etat est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ; « 5° L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire ; « L'autorité compétente qui transfère des données informe la Commission nationale de l'informatique et des libertés des transferts relevant du présent article. « L'autorité compétente garde trace de la date et l'heure de ce transfert, des informations sur le destinataire, et de la justification du transfert et les données à caractère personnel transférées. »	**données ne peut se faire que dans les conditions prévues par le code de procédure pénale.** ***Section 4*** ***Transferts de données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des Etats non membres de l'Union européenne*** ***Art. 70-25.*** **- Le responsable d'un traitement de données à caractère personnel ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées :** **1° Le transfert de ces données est nécessaire à l'une des finalités énoncées au 1° de l'article 70-1 ;** **2° Les données à caractère personnel sont transférées à un responsable dans cet Etat tiers ou à une organisation internationale qui est une autorité compétente chargée dans cet Etat des fins relevant en France du 1° de l'article 70-1 ;** **3° Si les données à caractère personnel proviennent d'un autre Etat, l'Etat qui**

			a transmis ces données a préalablement autorisé ce transfert conformément à son droit national. **Toutefois, si l'autorisation préalable ne peut pas être obtenue en temps utile, ces données à caractère personnel peuvent être retransmises sans l'autorisation préalable de l'Etat qui a transmis ces données lorsque cette retransmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre Etat ou pour la sauvegarde des intérêts essentiels de la France. L'autorité d'où provenaient ces données personnelles est informée sans retard.** **4° L'une au moins des trois conditions suivantes est remplie :** ***a)*** **La commission a adopté une décision d'adéquation en application de l'article 36 de la directive (UE) 2016/680 du Parlement et du Conseil du 27 avril 2016 ;** ***b)*** **A défaut d'une telle décision d'adéquation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement**

			contraignant ; ces garanties appropriées peuvent soit résulter des garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet Etat tiers, soit résulter de dispositions juridiquement contraignantes exigées à l'occasion de l'échange de données ; ***c)* A défaut d'une telle décision d'adéquation et de garanties appropriées telles que prévues au *b*, le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel ;** **Lorsque le responsable d'un traitement de données à caractère personnel transfère des données à caractère personnel sur le seul fondement de l'existence de garanties appropriées au regard de la protection des données à caractère personnel, autre qu'une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles, il avise la Commission nationale de l'informatique et des libertés des catégories de transferts relevant de ce fondement.** **Dans ce cas, le responsable du traitement des données doit garder**

			trace de la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et des données à caractère personnel transférées. Cette documentation est mise à la disposition de l'autorité de contrôle, sur sa demande. **Lorsque la commission a abrogé, modifié ou suspendu une décision d'adéquation adoptée en application de l'article 36 de la directive précitée, le responsable d'un traitement de données à caractère personnel peut néanmoins transférer des données personnelles ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ou s'il estime après avoir évalué toutes les circonstances du transfert qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.** ***Art. 70-26.*** **- Par dérogation aux dispositions de l'article précédent, le responsable d'un traitement de données à caractère personnel ne peut,**

			en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire : **1° A la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;** **2° A la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit ;** **3° Pour prévenir une menace grave et immédiate pour la sécurité publique d'un Etat membre de l'Union européenne ou d'un pays tiers ;** **4° Dans des cas particuliers, à l'une des finalités énoncées au 1° de l'article 70-1 ;** **5° Dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins.** **Dans les cas visés aux 4° et 5°, le responsable du traitement de données à caractère personnel ne transfère pas ces données s'il estime que les libertés**

			et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert envisagé. **Lorsqu'un transfert est effectué aux fins de la sauvegarde des intérêts légitimes de la personne concernée, le responsable du traitement garde trace de la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, et de la justification du transfert et les données à caractère personnel transférées. Il met ces informations à la disposition de la Commission nationale de l'informatique et des libertés, à sa demande.** ***Art. 70-27.*** **- Toute autorité publique compétente mentionnée au 2° de l'article 70-1 peut, dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un Etat n'appartenant pas à l'Union européenne, lorsque les autres dispositions de la présente loi applicables aux traitements relevant de l'article 70-1 sont respectées et que les conditions ci-après sont remplies :** **1° Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données**

			pour l'une des finalités énoncées à l'article 70-1 ; **2° L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas considéré ;** **3° L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre Etat est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ;** **4° L'autorité compétente de l'autre Etat est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ;** **5° L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire ;** **L'autorité compétente qui transfère**

			des données informe la Commission nationale de l'informatique et des libertés des transferts relevant du présent article. **L'autorité compétente garde trace de la date et l'heure de ce transfert, des informations sur le destinataire, et de la justification du transfert et les données à caractère personnel transférées.** Chapitre ~~XIII~~ **XIV** : Dispositions diverses […]
Titre IV ***Habilitation à mettre le droit national en conformité avec le droit européen de la protection des données personnelles***			
Article 20 *[Habilitation]*		I. - Dans les conditions prévues à l'article 38 de la Constitution, le Gouvernement est autorisé à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires : 1° A la réécriture de l'ensemble de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées des dispositions qui mettent le droit national en conformité avec le	

		règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et transposent la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, telles que résultant de la présente loi ; 2° Pour mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel, apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi, et abroger les dispositions devenues sans objet ; 3° A l'adaptation et aux extensions à l'outre-mer des dispositions prévues aux 1° et 2°, ainsi qu'à l'application en Nouvelle-Calédonie, à Wallis-et-Futuna en Polynésie française, à Saint-Barthélemy, à Saint-Pierre-et-Miquelon et dans les Terres australes et antarctique françaises. II. - Cette ordonnance est prise, après avis de la Commission nationale de l'informatique et des libertés, dans un délai de six mois à compter de la promulgation de la présente loi. III. - Un projet de loi de ratification est déposé devant le Parlement dans un délai de six mois à compter de la publication de l'ordonnance.	
Titre V			

Dispositions diverses et finales			
Article 21 (1°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 15*** Sous réserve des compétences du bureau et de la formation restreinte, la commission se réunit en formation plénière. En cas de partage égal des voix, la voix du président est prépondérante. La commission peut charger le président ou le vice-président délégué d'exercer celles de ses attributions mentionnées : - au troisième alinéa du I de l'article 23 ; - aux e et f du 2° de l'article 11 ; - au c du 2° de l'article 11 ; - au d du 4° de l'article 11 ; - aux articles 41 et 42 ; - à l'article 54 ; - aux deux derniers alinéas de l'article 69, à l'exception des traitements mentionnés aux I ou II de l'article 26 ;	La loi n°78-17 du 6 janvier 1978 relative à l'informatique et aux libertés est ainsi modifiée : 1° A l'article 15, le quatrième alinéa est supprimé ;	***Article 15*** Sous réserve des compétences du bureau et de la formation restreinte, la commission se réunit en formation plénière. En cas de partage égal des voix, la voix du président est prépondérante. La commission peut charger le président ou le vice-président délégué d'exercer celles de ses attributions mentionnées : ~~**- au troisième alinéa du I de l'article 23**~~ ; - aux e et f du 2° de l'article 11 ; - au c du 2° de l'article 11 ; - au d du 4° de l'article 11 ; - aux articles 41 et 42 ; - à l'article 54 ; - aux deux derniers alinéas de l'article 69, à l'exception des traitements mentionnés aux I ou II de l'article 26 ;

	- au premier alinéa de l'article 70.		- au premier alinéa de l'article 70.
Article 21 (2°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 16*** Le bureau peut être chargé par la commission d'exercer les attributions de celle-ci mentionnées : - au dernier alinéa de l'article 19 ; - à l'article 25, en cas d'urgence ; - au second alinéa de l'article 70.	2° A l'article 16, le troisième alinéa est supprimé ;	***Article 16*** Le bureau peut être chargé par la commission d'exercer les attributions de celle-ci mentionnées : - au dernier alinéa de l'article 19 ; ~~**- à l'article 25, en cas d'urgence ;**~~ - au second alinéa de l'article 70.
Article 21 (3°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 29*** Les actes autorisant la création d'un traitement en application des articles 25, 26 et 27 précisent : 1° La dénomination et la finalité du traitement ; 2° Le service auprès duquel s'exerce le droit d'accès défini au chapitre VII ; 3° Les catégories de données à caractère personnel enregistrées ;	3° A l'article 29, le mot : « 25, » est supprimé ;	***Article 29*** Les actes autorisant la création d'un traitement en application des articles ~~**25,**~~ 26 et 27 précisent : 1° La dénomination et la finalité du traitement ; 2° Le service auprès duquel s'exerce le droit d'accès défini au chapitre VII ; 3° Les catégories de données à caractère personnel enregistrées ;

	4° Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ; 5° Le cas échéant, les dérogations à l'obligation d'information prévues au V de l'article 32.		4° Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ; 5° Le cas échéant, les dérogations à l'obligation d'information prévues au V de l'article 32.
Article 21 (4°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 30*** I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent : 1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ; 2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions ; 3° Le cas échéant, les interconnexions,	4° Au I de l'article 30, le mot : « déclarations, » et les références à l'article 25 sont supprimées ;	***Article 30*** I. - Les ~~**déclarations,**~~ demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent : 1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ; 2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles ~~**25,**~~ 26 et 27, la description générale de ses fonctions ; 3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres

	les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ; 4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ; 5° La durée de conservation des informations traitées ; 6° Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ; 7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ; 8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ; 9° Les dispositions prises pour assurer la sécurité des traitements et des		formes de mise en relation avec d'autres traitements ; 4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ; 5° La durée de conservation des informations traitées ; 6° Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles ~~25,~~ 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ; 7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ; 8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ; 9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

	données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ; 10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5. Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum. II. - Le responsable d'un traitement déjà déclaré ou autorisé informe sans		10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5. Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum. II. - Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la commission : - de tout changement affectant les informations mentionnées au I ; - de toute suppression du traitement.

	délai la commission : - de tout changement affectant les informations mentionnées au I ; - de toute suppression du traitement.		
Article 21 (5°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 31*** I. - La commission met à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26. Cette liste précise pour chacun de ces traitements : 1° L'acte décidant la création du traitement ou la date de la déclaration de ce traitement ; 2° La dénomination et la finalité du traitement ; 3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté	5° Au I de l'article 31, les mots : « 23 à » sont remplacés par les mots : « 26 et » et les mots : « ou la date de la déclaration de ce traitement » sont supprimés ;	***Article 31*** I. - La commission met à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles ~~**23 à**~~ **26 et** 27, à l'exception de ceux mentionnés au III de l'article 26. Cette liste précise pour chacun de ces traitements : 1° L'acte décidant la création du traitement ~~**ou la date de la déclaration de ce traitement**~~ ; 2° La dénomination et la finalité du traitement ; 3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté

	européenne, celles de son représentant ; 4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ; 5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ; 6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne. II. - La commission tient à la disposition du public ses avis, décisions ou recommandations. III. - La Commission nationale de l'informatique et des libertés publie la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.		européenne, celles de son représentant ; 4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ; 5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ; 6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne. II. - La commission tient à la disposition du public ses avis, décisions ou recommandations. III. - La Commission nationale de l'informatique et des libertés publie la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.

Article 21 (6°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 39*** I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui	6° Au dernier alinéa de l'article 39, les mots : « ou dans la déclaration » sont supprimés ;	***Article 39*** I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas

	sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. II.-Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du		de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. II.-Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

	caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées. Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.		Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ~~**ou dans la déclaration**~~ adressée à la Commission nationale de l'informatique et des libertés.
Article 21 (7°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 67*** Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, et 39, le I de l'article 40 et les articles 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en œuvre aux seules	7° A l'article 67, sont supprimés : *a)* Au premier alinéa, les mots : « 22, les 1° et 3° du I de l'article 25, les articles » ; *b)* Le quatrième alinéa ; *c)* Au cinquième alinéa, les mots : « En cas de manquement constaté à ses devoirs, le	***Article 67*** Le 5° de l'article 6, les articles 8, 9, ~~**22, les 1° et 3° du I de l'article 25, les articles**~~ 32, et 39, le I de l'article 40 et les articles 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en œuvre aux seules fins :

	fins : 1° D'expression littéraire et artistique ; 2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession. Toutefois, pour les traitements mentionnés au 2°, la dispense de l'obligation de déclaration prévue par l'article 22 est subordonnée à la désignation par le responsable du traitement d'un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi. Cette désignation est portée à la connaissance de la Commission nationale de l'informatique et des libertés. En cas de non-respect des dispositions de la loi applicables aux traitements prévus par le présent article, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de se	correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés » ;	1° D'expression littéraire et artistique ; 2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession. **~~Toutefois, pour les traitements mentionnés au 2°, la dispense de l'obligation de déclaration prévue par l'article 22 est subordonnée à la désignation par le responsable du traitement d'un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi. Cette désignation est portée à la connaissance de la Commission nationale de l'informatique et des libertés.~~** En cas de non-respect des dispositions de la loi applicables aux traitements prévus par le présent article, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de se mettre en conformité avec la loi. **~~En cas de manquement constaté à ses devoirs, le correspondant est déchargé~~**

	mettre en conformité avec la loi. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés. Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.		~~de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.~~ Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.
Article 21 (8°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 70*** Si la Commission des Communautés européennes a constaté qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et	8° A l'article 70, les premier et troisième alinéas sont supprimés et au deuxième alinéa, les mots : « saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et » sont remplacés par les mots : « consultée en application de l'article 36 du règlement (UE) 2016/679 et en cas de transfert de données à caractère personnel vers cet Etat, la Commission	***Article 70*** ~~Si la Commission des Communautés européennes a constaté qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et~~

	faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données. Lorsqu'elle estime qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des Communautés européennes. Lorsqu'elle est saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et peut enjoindre au responsable du traitement de suspendre le transfert des données. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation		~~faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données.~~ Lorsqu'elle estime qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des Communautés européennes. Lorsqu'elle est ~~saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et~~ **consultée en application de l'article 36 du règlement (UE) 2016/679 et en cas de transfert de données à caractère personnel vers cet Etat, la Commission** peut enjoindre au responsable du traitement de suspendre le transfert des données. ~~Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé assure~~

	de la suspension du transfert. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet Etat.		~~un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet Etat.~~
Article 21 (9°) *[Mesures de coordination]* Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	***Article 71*** Des décrets en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi. L'avis rendu sur les décrets relatifs à l'application du I bis de l'article 22 et du 9° du I de l'article 25 est motivé et publié.	9° La deuxième phrase de l'article 71 est supprimée.	***Article 71*** Des décrets en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi. ~~L'avis rendu sur les décrets relatifs à l'application du I bis de l'article 22 et du 9° du I de l'article 25 est motivé et publié~~.
Article 22 *[Open data des traitements ayant fait*	.	Pour les traitements ayant fait l'objet de formalités antérieurement à l'entrée en vigueur de la présente loi, la liste mentionnée à l'article 31 de la loi n° 78-17 précitée, arrêtée à cette	

l'objet de formalités]		date, est mise à la disposition du public, dans un format ouvert et aisément réutilisable pour une durée de dix ans.	
Article 23 (1°) *[Disposition relative aux TAJ]* Code de procédure pénale	***Article 230-8*** Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de	L'article 230-8 du code de procédure pénale est ainsi modifié : 1° Le premier alinéa est remplacé par les dispositions suivantes : « Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui, d'office ou à la demande de la personne concernée, demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles fassent l'objet d'une mention. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce dans un délai de deux mois sur les suites qu'il convient de donner aux demandes qui lui sont adressées. La personne concernée peut former cette demande sans délai à la suite d'une décision devenue définitive de relaxe, d'acquittement, de condamnation avec dispense de peine ou dispense de mention au casier judiciaire, ou de non-lieu, ou décision de classement sans suite. Dans les autres cas, la personne ne peut former sa demande, à peine d'irrecevabilité, que lorsque ne figure plus aucune mention dans le bulletin n° 2 de son casier judiciaire. En cas de décision de relaxe ou d'acquittement, les données	***Article 230-8*** ~~**Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de non-lieu et**~~

	non-lieu et de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé. Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des	personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe, il en avise la personne concernée. Les décisions de non-lieu ou de classement sans suite, font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles ou ordonnant qu'elles fassent l'objet d'une mention sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé. » ; 2° Au troisième alinéa, les mots : « en matière d'effacement ou de rectification des données personnelles » sont supprimés. II. – Le premier alinéa de l'article 804 du même	~~de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.~~ **Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui, d'office ou à la demande de la personne concernée, demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles**

	conséquences sur la durée de conservation des données personnelles. Les décisions du procureur de la République en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction. Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.	code est ainsi rédigé : « Le présent code est applicable, dans sa rédaction résultant de loi n° xxx du xxx d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions : ».	**fassent l'objet d'une mention. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce dans un délai de deux mois sur les suites qu'il convient de donner aux demandes qui lui sont adressées. La personne concernée peut former cette demande sans délai à la suite d'une décision devenue définitive de relaxe, d'acquittement, de condamnation avec dispense de peine ou dispense de mention au casier judiciaire, ou de non-lieu, ou décision de classement sans suite. Dans les autres cas, la personne ne peut former sa demande, à peine d'irrecevabilité, que lorsque ne figure plus aucune mention dans le bulletin n° 2 de son casier judiciaire. En cas de décision de relaxe ou d'acquittement, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe, il en avise la personne concernée. Les décisions de non-lieu ou de classement sans suite, font l'objet d'une mention, sauf**

			si le procureur de la République ordonne l'effacement des données personnelles. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles ou ordonnant qu'elles fassent l'objet d'une mention sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé. Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la

			durée de conservation des données personnelles. Les décisions du procureur de la République **~~en matière d'effacement ou de rectification des données personnelles~~** sont susceptibles de recours devant le président de la chambre de l'instruction. Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.
Article 23 (2°) *[Disposition relative aux TAJ]* Code de procédure pénale	***Article 804*** Le présent code est applicable, dans sa rédaction résultant de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions : 1° Pour la Nouvelle-Calédonie et la Polynésie française, du cinquième alinéa de l'article 398 et des articles 529-3 à 529-6 ; 2° Pour les îles Wallis et Futuna, des	II. – Le premier alinéa de l'article 804 du même code est ainsi rédigé : « Le présent code est applicable, dans sa rédaction résultant de loi n° xxx du xxx d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions : ».	***Article 804*** **~~Le présent code est applicable, dans sa rédaction résultant de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions :~~** **Le présent code est applicable, dans sa rédaction résultant de loi n° xxx du xxx d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en**

	articles 52-1,83-1 et 83-2, du cinquième alinéa de l'article 398 et des articles 529-3 à 529-6.		**Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions :** 1° Pour la Nouvelle-Calédonie et la Polynésie française, du cinquième alinéa de l'article 398 et des articles 529-3 à 529-6 ; 2° Pour les îles Wallis et Futuna, des articles 52-1,83-1 et 83-2, du cinquième alinéa de l'article 398 et des articles 529-3 à 529-6.
Article 24 *[Dispositions d'entrée en vigueur de la présente loi]*		Les titres I[er] à III, et les articles 21 et 22 de la présente loi entrent en vigueur à compter du 25 mai 2018. Toutefois, les dispositions de l'article 70-15 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans leur rédaction résultant de l'article 19 de la présente loi et relatives à l'obligation de journalisation pourront entrer en vigueur à une date ultérieure ne pouvant excéder le 6 mai 2023 lorsqu'une telle obligation exigerait des efforts disproportionnés, et ne pouvant excéder le 6 mai 2026 lorsque, à défaut d'un tel report, il en résulterait de graves difficultés pour le fonctionnement du système de traitement automatisé. La liste des traitements concernés	

		par ces reports et les dates auxquelles, pour ces traitements, l'entrée en vigueur de cette obligation sera reportée seront déterminées par voie réglementaire.	