

**Délibération n° 2017-299 du 30 novembre 2017 portant avis
sur un projet de loi d'adaptation au droit de l'Union
européenne de la loi n°78-17 du janvier 1978**

(demande d'avis n°17023753)

La Commission nationale de l'informatique et des libertés,

Saisie par la ministre de la justice, garde des sceaux, d'une demande d'avis concernant un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 ;

Vu 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-4°-a) ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Isabelle FALQUE-PIERROTIN, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Émet l'avis suivant :

La Commission a été saisie, le 17 novembre 2017, d'un projet de loi 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, sur le fondement de l'article 11-4°-a) de cette même loi. En application de l'article 22 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes, cet avis sera rendu public.

Ce projet de loi a pour objet la mise en conformité du droit national avec le « paquet européen de protection des données » adopté par le Parlement européen et le Conseil le 27 avril 2016 qui se compose :

- **d'un Règlement (UE) 2016/679** (ci-après, « le Règlement ») relatif à la protection des personnes physiques à l'égard des données à caractère personnel, qui constitue le cadre général de la protection des données et est directement applicable à compter du 25 mai 2018 ;
- **d'une Directive (UE) 2016/680** relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière ou d'exécution de sanctions pénales (ci-après « la Directive »), qui doit être transposée au plus tard le 6 mai 2018.

Si la plupart des principes régissant le traitement de données à caractère personnel, posés par le législateur il y a près de 40 ans, restent valables, ce cadre juridique introduit un changement de paradigme.

Il repose en effet sur une logique de responsabilisation renforcée des acteurs, responsables de traitements et sous-traitants. Alors que la loi de 1978 reposait en grande partie sur une logique de « formalités préalables » (déclaration, autorisation, etc.), le Règlement repose sur une logique de conformité continue, tout au long du cycle de vie de la donnée, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur. En contrepartie de la réduction du contrôle en amont exercé via ces formalités, la Commission voit ses pouvoirs de contrôle et de sanction renforcés par la possibilité d'infliger des amendes allant, dans les cas les plus graves, jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires pour une entreprise.

Le Règlement renforce également les droits des personnes en facilitant l'exercice de ceux-ci et en créant de nouveaux droits, comme le droit à la portabilité des données personnelles ou un droit à l'oubli propre pour les mineurs.

Enfin, pour permettre une application uniforme et cohérente du Règlement, le législateur européen a prévu un mécanisme de coopération renforcée entre les autorités de protection des données, qui devront adopter des décisions communes lorsque les traitements de données seront transnationaux, dans le cadre du mécanisme dit du « guichet unique ».

L'adoption du « paquet européen de protection des données » constitue donc une avancée majeure. Ces textes doivent permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Ils constituent également un standard international en matière de protection des données, notamment compte tenu du champ d'application élargi du Règlement via le critère de ciblage.

Ces changements nécessitent d'adapter la loi fondatrice du 6 janvier 1978, que le projet choisit symboliquement de ne pas abroger, tout en conservant son article 1er.

Le projet de loi vise ainsi à modifier certains articles de la loi du 6 janvier 1978, soit pour les rendre compatibles avec le droit de l'Union (titre I), soit pour tirer parti des marges de manœuvre prévues par le Règlement (titre II), soit enfin pour transposer les dispositions de la Directive (titre III).

I. Observations d'ordre général

Sur le texte pris dans son ensemble, la Commission entend souligner deux apports substantiels du projet de loi soumis à son examen.

En premier lieu, la Commission souligne que, sur le fond, le projet qui lui est soumis remplit globalement l'objectif principal qui lui était assigné, à savoir adapter le droit français au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les opérateurs.

Il donne ainsi corps au nouveau Règlement, qui constitue une avancée considérable pour la protection des données à caractère personnel dans l'espace européen. Sous réserve des omissions relevées et des clarifications ou compléments proposés ci-après dans le cadre de l'examen article par article, le projet de loi dote en effet le régulateur des pouvoirs nécessaires à l'exercice de ses missions, dans un contexte marqué par la reconnaissance de nouveaux droits aux citoyens et le renforcement de la responsabilité des opérateurs. Il organise en outre l'articulation nécessaire des procédures internes aux nouveaux mécanismes européens de coopération.

En second lieu, la Commission se félicite de ce que le projet de loi mobilise de manière judicieuse les « marges de manœuvres » ouvertes aux Etats par le Règlement et soit ainsi en pleine cohérence avec la logique sous-tendant la démarche européenne.

Le Règlement comporte en effet plus d'une cinquantaine de renvois au droit national, permettant aux Etats membres de maintenir des formalités préalables à certains traitements, de poser des règles de fond propres ou de moduler les garanties offertes aux personnes. Il appartient au législateur national de se prononcer sur chacun de ces points, en décidant si et dans quelle mesure il souhaite faire usage de ces marges.

Si, sur certains points, la Commission pourra exprimer une appréciation divergente et proposera de positionner différemment le curseur, elle tient à souligner que, de manière globale, le projet de loi lui semble faire un usage raisonnable de ces marges, ne conservant une spécificité nationale que par exception, dans les cas qui le justifient absolument. Il s'inscrit ainsi pleinement dans la logique du Règlement, cadre unique et harmonisé pour l'ensemble des citoyens et opérateurs de l'espace européen.

Tout en soulignant ces deux apports du texte soumis à son examen, la Commission se doit d'attirer l'attention sur trois limites notables.

En premier lieu, la Commission regrette le calendrier retenu pour l'adaptation du droit français. Si elle a été associée en amont, par le ministère de la justice, aux réflexions sur cette entreprise législative, elle déplore d'avoir été saisie aussi tardivement du projet et de ne pas avoir disposé du délai nécessaire à l'examen, dans des conditions acceptables, d'un texte d'une telle portée.

Surtout, la Commission souligne le risque réel de non-respect des délais de mise en œuvre du « paquet européen », qui doit impérativement être en application à compter du 6 mai 2018 pour ce qui concerne la Directive et du 25 mai 2018 pour ce qui concerne le Règlement.

Tenir ce calendrier n'est pas seulement un enjeu juridique : il s'agit d'un enjeu opérationnel majeur, la mise en œuvre effective des mécanismes de coopération prévus par le Règlement pouvant être compromise en l'absence de textes nécessaires, ainsi que d'un enjeu de crédibilité politique tant la France, par la voix notamment de la Commission a, aux niveaux national et européen, promu ces nouveaux instruments. Le respect de ces délais suppose l'adoption et l'entrée en vigueur impératives, avant les dates indiquées ci-dessus, non seulement du présent projet de loi, mais aussi des textes subséquents devant venir le compléter au niveau réglementaire, à savoir le(s) nécessaire(s) décret(s) d'application et une modification du règlement intérieur de la Commission.

En deuxième lieu, la Commission dénonce le défaut de lisibilité de l'état du droit résultant du projet de loi.

Cette complexité est pour partie inévitable en raison du choix fait par le législateur européen lui-même d'adopter un Règlement et une Directive. De ce choix découle pour les citoyens la nécessité de combiner la lecture du Règlement, qui ne nécessite formellement aucune mesure de transposition en droit interne et ne peut d'ailleurs être recopié par des textes nationaux, et d'un certain nombre de dispositions nationales, prises au titre des marges de manœuvre du Règlement, pour la transposition de la Directive ou pour les traitements situés en dehors du champ de l'un comme de l'autre. Cette combinaison d'un Règlement et de textes nationaux remplacera le corpus unique que constitue aujourd'hui la loi de 1978.

La Commission constate cependant que ce premier degré de complexité, inévitable, se trouve aggravé par les choix légistiques retenus, à ce stade, au niveau interne. En effet, le Gouvernement a fait le choix de n'opérer que les modifications strictement indispensables, sur le fond, à la mise en œuvre du Règlement et de la Directive, et de renvoyer la réécriture d'ensemble de la loi du 6 janvier 1978 à une ordonnance ultérieure, conformément à l'habilitation prévue à l'article 23 du projet de loi.

Or, dans l'attente de cette ordonnance, ce choix induit une double difficulté de lecture. D'une part, la loi pourra induire en erreur le lecteur sur la portée de ses droits et obligations. En effet, des dispositions formellement inchangées et toujours en vigueur de la loi de 1978 ne seront en réalité plus applicables, car substituées, dans leur champ, par les dispositions du Règlement (par exemple sur le consentement, la base légale des traitements ou la portée des droits reconnus aux personnes), tandis que la loi nationale ne comportera aucun écho à certains nouveaux droits ou nouvelles obligations posés par le Règlement.

D'autre part, la loi du 6 janvier 1978 ne donnera pas de grille de lecture permettant aux citoyens et aux responsables de traitement de comprendre les droits et obligations différenciés qui existeront demain dans les trois grands compartiments de la protection des données que seront le champ du Règlement (à savoir les fichiers « civils et commerciaux », mais également certains fichiers relevant de l'administration), celui de la Directive (traitements à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites) et, enfin, ce qui ne relève pas du champ du droit de l'Union ou relève du seul chapitre 2 du titre V du traité sur l'Union européenne (traitements intéressant la sûreté de l'Etat et la défense).

Un dernier enjeu de lisibilité tient aux difficultés de frontière, que le projet de loi ne saurait d'ailleurs résoudre à lui seul, qui se poseront entre les différents régimes applicables aux traitements de données selon leurs finalités, parfois multiples, certains traitements pouvant relever du Règlement et de la Directive, d'autres relevant à la fois du champ de la Directive et du « hors-champ » du droit de l'Union.

Cet enjeu de lisibilité dépasse la seule structuration technique du texte. Il conditionne la pleine effectivité des droits des citoyens et des obligations des différents acteurs. Le choix fait est d'autant plus dommageable que la loi du 6 janvier 1978 constitue, par son objet et par son rayonnement aux niveaux européen et international, l'un des grands marqueurs du droit français, connu et pris comme standard.

La Commission appelle dès lors de ses vœux l'adoption des plus rapprochées de l'ordonnance annoncée, ainsi qu'une réécriture du droit français conforme aux principes ci-dessus, de manière à ce que la loi du 6 janvier 1978 puisse donner un mode d'emploi clair, ce qui est démocratiquement l'une de ses vocations.

En troisième et dernier lieu, la Commission regrette que, compte tenu notamment du calendrier retenu, le projet de loi constitue à certains égards une occasion manquée de procéder à un réexamen global du droit de la protection des données en France, de compléter le dispositif législatif sur certains points et d'approfondir les droits des personnes pour les traitements entrant dans le champ de la Directive ainsi que pour ceux situés en dehors du champ du droit de l'Union.

Autant il est nécessaire, dans le champ du Règlement, de s'inscrire, compte tenu de la nature de ce texte, dans la logique d'harmonisation de celui-ci, autant le Gouvernement pouvait s'interroger, en dehors du champ du Règlement, sur l'opportunité de retenir un niveau d'ambition supérieur au socle minimal que constitue la Directive.

Dans le champ de la Directive en particulier, si la Commission se félicite du maintien d'une autorisation de mise en œuvre de tels traitements par acte réglementaire pris après son avis publié et motivé, elle relève que le projet de loi n'apporte aucune garantie supérieure à ce que prévoit la Directive, alors que même le droit national et sa pratique ont permis la mise en œuvre de telles garanties, qu'il conviendrait de faire figurer expressément dans ces dispositions spéciales. S'agissant des traitements ne relevant pas du champ du droit de l'Union, la Commission estime regrettable que les garanties prévues par la Directive précitée ne leur soient pas rendues applicables, alors même qu'elles permettraient d'accroître le niveau de protection des données traitées notamment dans le cadre de la sûreté de l'Etat sans affecter pour autant l'exercice des missions des autorités compétentes. La Commission estime que le législateur pourrait utilement intervenir sur ces points.

II. Examen article par article

TITRE I^{ER}

DISPOSITIONS COMMUNES AU REGLEMENT ET A LA DIRECTIVE 2016

CHAPITRE I^{ER}

DISPOSITIONS RELATIVES A LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

Article 1^{er} (Missions de la Commission)

Cet article, particulièrement important, vise à compléter les missions de la Commission pour tenir compte du nouvel environnement juridique, qui implique qu'elle doive s'inscrire, plus encore qu'aujourd'hui, dans une logique d'accompagnement des acteurs, eux-mêmes davantage responsabilisés et donc davantage demandeurs de sécurité juridique. Sont ainsi prévus l'établissement par la Commission d'outils destinés à faciliter la mise en conformité et l'évaluation préalable des risques par les acteurs ; l'encouragement de la production de codes de conduite ; l'élargissement du périmètre des mécanismes de certification et des précisions sur les règlements types de sécurité. Le projet prévoit en outre que la Commission peut être consultée par le Président des deux chambres sur toute proposition de loi relative à la protection des données.

- La Commission souligne le grand intérêt des dispositions du a) bis introduit dans l'article 11 de la loi du 6 janvier 1978 par le projet de loi, qui lui permettront de convertir son patrimoine normatif actuel (autorisations uniques, normes simplifiées, etc.) dans le nouvel environnement juridique sous la forme de référentiels, lignes directrices et recommandations notamment.

Par ce biais, la réduction des formalités préalables ne privera pas le régulateur d'outils de régulation efficaces permettant de guider les acteurs dans leurs démarches de conformité, en leur donnant, par des outils de droit souple ou d'interprétation de l'état du droit, une indication sur ce que le régulateur estime conforme à la loi ou au Règlement à un moment donné. Ces référentiels pourront être pris en compte, le cas échéant, dans la mise en œuvre par les responsables de traitements de leur obligation de réaliser une analyse d'impact préalable – soit pour orienter les hypothèses de dispense d'analyse d'impact, soit pour guider la confection de ces analyses. Dans ce dernier cas, le niveau de risque pourra être réputé acceptable si le traitement envisagé est conforme au référentiel ; en revanche, si le traitement s'écarte du référentiel, l'analyse d'impact devra être soumise à la Commission.

La Commission relève toutefois que l'article relatif aux missions fait référence à « *la présente loi et au Règlement (UE) 2016/679* ». Elle estime nécessaire de viser plus largement « les textes relatifs à la protection des données à caractère personnel » dans la mesure où d'autres textes sont susceptibles de trouver application, tels que le futur Règlement dit « e-privacy », et nécessiter l'élaboration de référentiels.

- La Commission souscrit également à la possibilité, prévue par la rédaction projetée du b) de l'article 11 de la loi du 6 janvier 1978 modifiée, d'élaborer des « règlements types », au titre notamment des conditions supplémentaires ou des garanties que le droit national peut introduire pour le traitement des données biométriques, génétiques et de santé ou pour les données d'infractions.

La Commission regrette toutefois qu'ils ne puissent concerner les traitements mis en œuvre pour le compte de l'Etat, agissant dans l'exercice même des prérogatives de puissance publique, alors que le besoin de cadrage du traitement de certaines données n'y est pas moins important.

Elle regrette également que l'objet de ces règlements-types soit limité à la seule dimension de la sécurité des systèmes. En effet, d'autres dimensions de la protection des données (finalité, minimisation des données, respect des droits, etc.) devraient pouvoir faire l'objet d'un encadrement par des règles de fond, et non seulement par des règles de sécurité, dans le respect des marges de manœuvre permises par le Règlement, notamment par son article 9.4. Faute de disposer de la possibilité d'adopter des règles contraignantes – alors qu'elle dispose d'ores et déjà d'un pouvoir réglementaire, via par exemple ses autorisations uniques – la Commission ne pourra tout au plus qu'émettre des recommandations. Or, s'agissant de données aussi sensibles, des instruments de « droit dur » s'avèreraient plus protecteurs des droits des personnes et plus sûrs pour les opérateurs, en affichant clairement les frontières entre le permis et l'interdit.

La Commission, par ailleurs consciente du risque d'une inadéquation rapide entre le contenu de ces règlements et la réalité d'un secteur concerné, et du danger de trop grandes disparités entre la France et les autres pays européens qui n'encadreraient pas de manière aussi stricte certaines catégories de traitement, estime dès lors que de tels instruments devraient être prévus, dont elle ferait naturellement un usage raisonné.

- Concernant le recours aux mécanismes de certification, les pouvoirs de la Commission sont explicités dans un nouveau paragraphe f bis) du 2° de l'article 11 sans faire de lien avec l'actuel c) du 3° qui concerne la délivrance actuelle des labels, qu'il conviendrait de supprimer tout en réinjectant dans le texte la possibilité de délivrer des labels et marques. Ces modifications permettraient de donner une identité visuelle à la certification des personnes, produits, systèmes ou procédures, destinée à démontrer la conformité avec le Règlement et la loi. Le projet de loi pourrait toutefois être complété, à titre de clarification, pour indiquer que la Commission peut, dans l'exercice de son pouvoir de fixation des règles d'agrément, établir « des exigences supplémentaires au référentiel d'accréditation du Cofrac ».

- La Commission estime enfin que le projet de loi devrait être complété de la possibilité pour la Commission de participer aux instances européennes et internationales compétentes en matière de protection des données. Ainsi, la participation de la Commission au Comité européen de protection des données (CEPD), à la fois dans le contexte du Règlement et de la Directive, devrait être expressément prévue, ainsi que la possibilité plus large de participer aux instances internationales. En effet, la loi actuelle ne prévoit cette possibilité que sur demande du Premier ministre, à l'article 11-4°-d), ce qui s'est révélé insuffisant et inadapté à la fréquence des réunions.

Article 2 (Composition de la Commission) et 3 (Commissaire du Gouvernement)

Les clarifications ou précisions apportées par ces deux articles n'appellent pas d'observation.

Article 4 (Pouvoirs de contrôle de la Commission)

L'article 4 du projet de loi a pour objet de modifier l'article 44 de la loi du 6 janvier 1978 qui porte sur les pouvoirs de la Commission en matière de contrôle. Cet article, essentiel pour le bon fonctionnement des nouveaux mécanismes de contrôle conjoint et pour la bonne application du Règlement, appelle les remarques suivantes.

- Le 1° et le 2° de l'article 4 permettent aux agents habilités de la Commission de contrôler la mise en œuvre de traitement dans des locaux qui n'ont ni le caractère de local professionnel, ni celui de domicile privé, tels que des parties communes d'immeubles. Cette disposition apporte à la compétence de contrôle de la Commission un complément bienvenu pour la pleine et entière application du Règlement.

- Le 3° du même article précise les conditions de recueil, par les agents habilités de la Commission, des éléments nécessaires à l'exercice de leur mission de contrôle (documents, données, renseignements divers, etc.), en modifiant l'actuelle rédaction du III de l'article 44 de la loi du 6 janvier 1978. Le projet de loi prévoit d'importantes clarifications sur les droits et parties prenantes au contrôle, en particulier sur l'opposabilité des secrets protégés par la loi, ainsi que le permet l'article 90 du Règlement.

La rédaction retenue par le projet appelle cependant de la Commission trois séries d'observations, qui portent sur la rédaction projetée de l'alinéa 1^{er} de l'article 44-III de la loi.

- En premier lieu, il est prévu que les membres et agents de la Commission « *peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles.* » Or, une telle rédaction pourrait être interprétée comme laissant aux organismes contrôlés la possibilité de s'opposer au recueil de document par la Commission lorsque les missions de contrôle ne sont pas opérées sur place ou sur convocation, c'est-à-dire sur pièce ou en ligne. Les mots « sur place et sur convocation » devraient dès lors être introduits par un « notamment » pour englober l'ensemble des modalités de contrôle.

- En deuxième lieu, le même alinéa prévoit que les membres et agents de la Commission « *peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données [...]* ». Cette disposition met en exergue la nécessité pour la Commission de prendre toutes les précautions utiles lorsqu'elle réalise des contrôles, à savoir de veiller en particulier à la sécurité des données collectées. A cet égard, la Commission souligne que de telles mesures sont d'ores et déjà mises en œuvre par les agents habilités à procéder à des vérifications qui sont en outre astreints au secret professionnel pour les faits, actes et

renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues par le code pénal.

- En troisième lieu, il est prévu que le secret ne peut être opposé aux membres et agents de la Commission, « *sauf concernant les informations couvertes, par le secret de l'enquête et de l'instruction, 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.* » Cette modification apporte une clarification bienvenue des conditions d'opposabilité à la Commission des différents secrets protégés par la loi.

Néanmoins, la mention du « *secret de l'enquête et de l'instruction* » ne saurait être interprétée comme s'opposant au contrôle, par la Commission, des traitements utilisés par les autorités judiciaires ou services de police judiciaire, dès lors que sa mission de contrôle n'interfère pas avec ces secrets. A défaut, cette mention devrait être supprimée pour éviter toute difficulté opérationnelle pour la Commission dans le champ de la Directive et pour prévenir toute invocation de ce secret à des fins dilatoires en dehors des cas pour lesquels il est prévu par le code de procédure pénale.

A titre plus général, la Commission rappelle que le Règlement comme la Directive ne lui donnent pas compétence pour « *contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle* » (articles 55 du Règlement et 45 de la Directive). Ces dispositions visent à préserver les juridictions de toute interférence liée à la protection des données dans leur activité, leurs procédures et leurs prérogatives en matière de collecte de données nécessaires à ces procédures. En revanche, elles ne sauraient faire obstacle à la mise en œuvre de la compétence de la Commission sur les traitements extérieurs aux dossiers de procédure et utilisés dans le cadre de ces missions (Cassiopée, Fnaeg, etc.), ni, au demeurant, aux vérifications qu'implique la mise en œuvre du droit d'accès indirect prévu à l'article 41 de la loi.

Article 5 (Coopération)

Les nouveaux articles 49-1, 49-2, 49 ter et quater, introduits dans la loi du 6 janvier 1978 par l'article 5 du projet de loi, ont pour objet de préciser les modalités de coopération entre la CNIL et les autorités de protection des données des autres Etats membres de l'Union. Ils appellent de la Commission les observations suivantes.

- Le projet doit tout d'abord être complété en ce qui concerne la saisine du Comité européen à la protection des données.

La mise en œuvre des actions de coopération, dont les principes sont établis aux articles 60, 61 et 62 du Règlement, peut en effet conduire les autorités de contrôle à adopter des décisions pouvant relever, en France, soit du pouvoir du Président de la Commission (décision de contrôle, clôture de plainte, mise en demeure), soit de la formation restreinte (décision de sanction). Dans ce cadre, les différents organes de la Commission devraient être en mesure, en cas de désaccord entre autorités nationales, de saisir le Comité européen, ainsi que le prévoit l'article 65 du Règlement.

La Commission relève que le projet de loi prévoit expressément que lorsque la CNIL est autorité chef de file, la formation restreinte peut, le cas échéant, saisir le CEPD après avoir soumis son projet de décision aux autorités concernées et s'être prononcée

sur leurs objections pertinentes et motivées (second alinéa du projet d'article 49 ter). En revanche, une telle faculté n'a pas été prévue au titre des pouvoirs du Président de la Commission. Le projet devrait dès lors être amendé en ce sens.

- La Commission souligne ensuite l'opportunité de compléter le projet s'agissant du respect du contradictoire dans le cadre de la procédure devant la formation restreinte lorsque la CNIL est autorité chef de file au sens du Règlement.

Le projet d'article 49 ter décrit la procédure suivie devant la formation restreinte lorsque la Commission est chef de file (la communication du rapport et de toute information utile aux autorités de contrôle concernées, la possibilité pour celles-ci d'assister à la séance, la prise en compte des objections pertinentes et motivées des autorités concernées etc.). Qu'il y ait ou non saisine du CEPD, la décision finale de la formation restreinte peut varier du projet de décision initial, s'il a été tenu compte d'objections formulées par les autres autorités concernées. Ainsi, les manquements retenus ou la mesure prononcée pourraient ne pas correspondre au périmètre du rapport de sanction sur lequel le responsable ou le sous-traitant s'est défendu.

En conséquence, la Commission estime utile d'insérer dans le projet de loi une disposition précisant que les conditions dans lesquelles le caractère contradictoire de la procédure est garanti à l'égard de l'organisme concerné seront définies par voie réglementaire.

- La Commission attire enfin l'attention sur la nécessité de modifier les dispositions relatives aux pouvoirs d'enquête détenus par les membres et agents des autres autorités de contrôle nationales.

Le projet de loi crée un article 49-1-II qui porte sur les opérations de contrôle conjointes mises en œuvre en application du Règlement, qui peuvent notamment prendre la forme d'enquêtes effectuées dans les locaux des responsables de traitement. La rédaction de cet article emporte à certains égards des conséquences sur les contrôles opérés par la Commission en coopération avec une autre autorité de protection des données.

Le dernier alinéa du projet d'article 49-1-II dispose que « *Les pouvoirs d'enquête exercés par les membres et agents des autres autorités de contrôle se limitent à une présence aux côtés des membres et agents de la Commission nationale de l'informatique et des libertés participant à l'opération de contrôle. [...]* ». Or, une telle rédaction cantonne les membres et agents d'autres autorités à un rôle de simple observateur, ce qui induit, en pratique, qu'ils ne sauraient poser des questions à l'organisme contrôlé, retirant ainsi l'effet utile du contrôle conjoint entre autorités. La Commission relève que la réalisation d'opérations conjointes constitue la forme la plus aboutie de coopération et implique un haut niveau d'implication des autorités participantes et estime dès lors qu'en ne créant pas les conditions opérationnelles nécessaires à la réalisation de l'objectif d'une coopération efficace entre autorités, le projet de loi s'écarte de l'esprit de l'article 62-3 du Règlement.

Ainsi, la Commission propose, d'une part, de conserver dans le texte le principe d'une participation des agents des autres autorités de contrôle aux investigations menées par la CNIL à l'occasion d'opérations conjointes et, d'autre part, de renvoyer au Président de la Commission le soin de fixer, dans la décision d'habilitation à procéder à des

vérifications, le périmètre de leurs pouvoirs d'enquêtes, qui ne sauraient en tout état de cause excéder ceux dont dispose un agent de la CNIL. Par ailleurs, les agents des autres autorités de contrôle ne sauraient agir que sous le contrôle de la Commission. Elle rappelle à cet égard que d'autres législations nationales (notamment en Suède et en Espagne) doivent prévoir la possibilité pour des agents d'autres autorités de contrôle de participer à des missions de contrôle en leur conférant des pouvoirs d'investigation équivalents à ceux de leurs propres agents.

Article 6 (Mesures correctrices)

L'article 6 du projet de loi traite des mesures correctrices visées au 2 de l'article 58 du Règlement que la CNIL peut prendre en cas de méconnaissance par le responsable de traitement et le sous-traitant de ses obligations issues de la loi ou du Règlement.

Il a ainsi pour objet de modifier les articles 45 à 48 de la loi du 6 janvier 1978 et de répartir ces mesures correctrices entre le Président de la CNIL et la formation restreinte. Il traite également des types de procédure en urgence et hors urgence. Il clarifie, dans le sens de l'article 83 du Règlement, les hypothèses dans lesquelles la formation restreinte peut prendre une sanction sans mise en demeure préalable. Le projet de loi procède ainsi à une adaptation nécessaire du droit national au Règlement, ce dernier comportant une liste unique de mesures correctrices sans préjuger de l'organisation interne de chaque autorité de contrôle nationale. La ventilation retenue par le projet de loi n'appelle de la part de la Commission que les observations suivantes.

- En premier lieu, la Commission relève que le 2° du II de l'article 45 de la loi modifiée dispose que la formation restreinte de la CNIL peut prononcer une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du Règlement, assortie, sauf dans le cas où le traitement est mis en œuvre par l'Etat, d'une astreinte. La Commission considère que l'injonction sous astreinte constitue une mesure efficace permettant d'emporter des effets dissuasifs à l'égard de responsables de traitement ou de sous-traitants et de garantir l'effectivité de leurs obligations ainsi que des droits des personnes. L'usage de ce nouveau pouvoir devrait correspondre aux hypothèses mentionnées, s'agissant de l'Autorité de la concurrence, à l'article L. 464-2 du code de commerce et les conditions de recours à l'astreinte pourraient, le cas échéant, être précisées expressément dans le projet de loi.

Elle regrette, cependant, qu'une telle injonction avec astreinte ne soit pas également prévue afin de satisfaire aux demandes présentées par les personnes en vue d'exercer leurs droits (accès, opposition ou rectification notamment). Or, les deux tiers des plaintes dont est saisie la Commission chaque année portent sur l'exercice d'un droit et, dans de nombreux cas, un pouvoir d'injonction avec astreinte permettrait de satisfaire aux demandes des plaignants. Ce pouvoir d'injonction devrait être prévu pour garantir l'effectivité des droits conférés aux citoyens par le Règlement.

- En deuxième lieu, le 3° du III de l'article 45 de la loi modifiée dispose que le Président de la CNIL peut mettre en demeure de communiquer à la personne concernée une violation de données à caractère personnel « à l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense et ceux mentionnées à l'article 27 ». Une telle mesure peut donc en revanche être prononcée s'agissant des traitements visés au 2° du I de l'article 26 de la même loi, conformément à ce que prévoit le c° du II de l'article 47 de la Directive.

La Commission estime qu'afin d'être en mesure d'assurer le plus haut niveau de protection des droits, l'obligation de communiquer à la personne concernée une violation de données à caractère personnel devrait, par principe, s'étendre à tous les traitements sans exception. Elle considère en outre que l'enjeu d'information des personnes concernées est d'autant plus crucial que les conséquences d'une divulgation de données pour elles sont importantes, ce qui peut être le cas des traitements mentionnés à l'article 27 de la loi du 6 janvier 1978.

- En troisième lieu, il est prévu quatre types d'exception au titre des pouvoirs dont dispose la formation restreinte en application des articles 45 et 46 de la loi modifiée. L'articulation entre ces différentes exceptions et leurs modalités de mise en œuvre n'apparaît pas toujours suffisamment cohérente.

La Commission relève tout d'abord que le 3° du II du projet d'article 45 prévoit la limitation temporaire ou définitive du traitement ou son interdiction, à « *l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense* » visés au 1° du I de l'article 26 de la loi. La Commission en déduit que les mesures de limitation ou d'interdiction seraient applicables aux autres traitements relevant des articles des articles 26 et 27. En revanche, en application du 1° du I de l'article 46 tel que modifié par le projet de loi, la formation restreinte ne pourrait pas, pour ces mêmes traitements, prononcer une interruption provisoire de leur mise en œuvre en cas d'urgence et d'atteinte aux droits et libertés visés à l'article 1^{er} de la loi.

Dans un souci de cohérence et pour assurer le plus haut niveau de protection des droits des personnes, la Commission considère que la formation restreinte devrait également pouvoir prononcer une interruption provisoire de la mise en œuvre desdits traitements lorsque les conditions sont réunies. A défaut, la formation restreinte disposerait en urgence de pouvoirs inférieurs à ses pouvoirs ordinaires.

Ensuite, le projet de loi dispose au 7° du I du projet d'article 46 que la formation restreinte peut informer le Premier ministre afin qu'il prenne des mesures correctrices s'agissant des traitements mentionnés aux I et II de l'article 26 de la loi du 6 janvier 1978. Il apparaît en revanche que l'information du Premier ministre est exclue s'agissant des traitements relevant de l'article 27 de la même loi. De la même manière, le 2° du I de l'article 46 de la loi modifiée prévoit la possibilité de limiter provisoirement le traitement de certaines données « *si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et II de l'article 26* ». La Commission en déduit que la limitation provisoire des données est possible pour les traitements relevant de l'article 27.

Là encore, dans un souci de cohérence et pour assurer le plus haut niveau de protection des droits des personnes, la Commission considère que la formation restreinte devrait pouvoir, d'une part, informer le Premier ministre afin qu'il prenne des mesures correctrices s'agissant des traitements relevant de l'article 27 et, d'autre part, limiter provisoirement le traitement de certaines données de traitements mentionnés au I et II de l'article 26.

- En quatrième et dernier lieu, la Commission souligne l'intérêt qui s'attacherait à ce qu'une plus grande souplesse organisationnelle soit laissée à la formation restreinte. L'actuel article 13 de la loi du 6 janvier 1978 dispose que la formation restreinte est composée d'un Président et de cinq membres, sans ouvrir expressément au pouvoir

réglementaire la possibilité de prévoir l'adoption de certaines décisions dans des formats plus resserrés. Or, le Règlement va conduire à un accroissement significatif du nombre et du type d'actes relevant de la compétence de la formation restreinte (formulation d'objections, saisine du CEPD notamment). Ces nouveaux objets de décision vont s'ajouter à un spectre d'ores et déjà très large d'affaires, allant de cas simples (refus de satisfaire à une demande individuelle d'exercice d'un droit) à des cas plus complexes (violations de données à grande échelle).

Dès lors, il apparaîtrait opportun de permettre soit au président de la formation restreinte seul, soit à une fraction resserrée de celle-ci, de prononcer certaines catégories de mesures, en particulier des sanctions de faible montant ou des décisions européennes de pure procédure.

Enfin, la Commission note que la nouvelle loi pourrait constituer une opportunité de modifier le nom de la formation restreinte (au profit de celui, par exemple, de formation des sanctions).

CHAPITRE II

DISPOSITIONS RELATIVES A CERTAINES CATEGORIES DE DONNEES

Article 7 (Données sensibles)

L'article 7 modifie la rédaction actuelle de l'article 8 de la loi du 6 janvier 1978 en vue de la mettre en cohérence avec les dispositions du paragraphe 1 de l'article 9 de Règlement. Il reprend donc le principe d'interdiction de traitement des données sensibles et élargit le champ de ces données par rapport à la rédaction actuelle de l'article 8 (ajout des données biométriques, génétiques et des données concernant l'orientation sexuelle des personnes).

- La Commission entend d'abord souligner des difficultés tenant à l'articulation entre champs du Règlement et de la Directive. Cet article du projet de loi figure en effet dans les dispositions communes à l'ensemble des traitements, y compris ceux relevant de ces deux instruments, soumis à la loi (titre 1er).

Or, la Directive ne retient pas les mêmes principes pour le traitement des données sensibles. En effet, si l'article 10 de la Directive a un champ d'application identique en ce qui concerne les données, il prévoit que le traitement de données sensibles 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 ; / 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 »*.

Dès lors, la Commission considère que la rédaction proposée n'est pas conforme à la Directive. Si, pour les traitements relevant du Règlement, il est fait application directe de l'article 9 dudit texte pour le principe d'interdiction de traitement de ces données, il est nécessaire de prévoir une disposition pour transposer les principes énoncés à

l'article 10 de la Directive et de circonscrire l'adoption de dispositions nationales destinées à mettre en œuvre le Règlement au champ de cet instrument.

Par ailleurs, se pose la question du traitement de données sensibles qui sont hors du champ d'application du Règlement et de la Directive (par exemple, pour les traitements intéressant la défense et la sûreté de l'État). La Commission considère qu'un régime identique à celui prévu par la Directive pour ce type de traitements serait cohérent et plus protecteur.

- Par ailleurs, du fait que les données biométriques sont des données sensibles, leur traitement ne peut être autorisé que dans les conditions mentionnées à l'article 9.2 du Règlement. Ainsi un traitement de données biométriques peut notamment être justifié par un motif d'intérêt public important (g) ou par le fait que la personne concernée a donné son consentement explicite (a). Ils peuvent également être mis en œuvre si « *le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail (...) dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée* » (b).

Au regard de ces dispositions, le seul intérêt légitime du responsable de traitement ne saurait désormais servir de fondement à la mise en œuvre d'un tel traitement.

Or, la Commission relève que les employeurs peuvent, en l'état du droit, mettre en place des dispositifs biométriques concernant leurs employés après autorisation de la Commission, sur le seul fondement de leur intérêt légitime. Compte tenu du nombre important de demandes, la Commission a adopté plusieurs autorisations uniques en la matière, relatives à l'usage de la biométrie pour le contrôle d'accès aux lieux de travail, sous réserve de la mise en œuvre de garanties de protection des données suffisantes.

Dans la mesure où le Règlement ne rend plus possible le recours au seul intérêt légitime, la Commission souligne que la poursuite de ces traitements au-delà du 25 mai 2018 n'apparaît pas sécurisée.

En effet, il n'est tout d'abord pas évident, dans tous les cas de figure, de se fonder sur la base légale du consentement des personnes dans le contexte particulier d'un traitement mis en œuvre par un employeur sur les données de ses employés. Par ailleurs, le motif tiré des « *obligations et de l'exercice des droits propres au responsable du traitement [...] en matière de droit du travail* » suppose, d'une part, la démonstration de la « nécessité » du traitement des données biométriques et requiert, d'autre part, l'existence dans le droit de l'Union ou dans le droit national d'une base légale « autorisant » un tel traitement de données à caractère personnel. Or, l'existence d'une telle base n'apparaît pas établie à ce stade de l'examen du texte.

Par suite, la Commission appelle l'attention du Gouvernement et du législateur sur la nécessité, s'il est souhaité de permettre la poursuite de ces traitements, de prévoir dès à présent, *a minima*, une base légale appropriée. Celle-ci pourrait soit figurer de manière pérenne dans le projet de loi lui-même, soit prendre la forme, à court terme, d'une disposition transitoire permettant, en des termes suffisamment spécifiques, la

poursuite des traitements compatibles avec l'article 9.2.(b) du Règlement jusqu'au passage en revue, dans un délai fixé à l'avance, de l'ensemble de la législation interne.

Dans cette optique, les décisions d'autorisation adoptées ces dernières années par la Commission pourraient offrir un éclairage au législateur et au pouvoir réglementaire, y compris dans le cadre de règlements types, quant aux garanties à mettre en œuvre pour s'assurer de l'intégration des principes de protection des données personnelles par défaut et dès la conception des dispositifs biométriques.

TITRE II

MARGES DE MANOEUVRE

CHAPITRE I (CHAMP D'APPLICATION)

Article 8 (Champ d'application territorial)

L'article 8 du projet de loi vient préciser le champ d'application de la loi nationale. Il prévoit qu'en cas de divergence de législations entre Etats membres liée aux marges de manœuvre laissées par le Règlement, la loi nationale s'applique dès lors que la personne réside en France et ce, même si le responsable de traitement n'est pas établi en France. La logique est en revanche inversée dans le cadre du respect du droit à la liberté d'expression et d'information, par exemple dans le domaine de la presse, où le droit applicable est celui de l'Etat dans lequel est établi le responsable.

La Commission prend acte de ces dispositions, tout en soulignant les difficultés opérationnelles qui pourraient naître avec les pays ayant retenu des critères différents et incompatibles avec ceux retenus par le projet de loi.

CHAPITRE II

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

Article 9 (Formalités et NIR)

Le chapitre II du projet de loi, qui contient un unique article 9, vise à simplifier les formalités préalables à la mise en œuvre des traitements. A ce titre, il supprime l'ensemble des formalités préalables jusqu'ici imposées par la loi, à savoir l'obligation de déclaration ou d'autorisation auprès de la Commission, à l'exception des traitements dans le domaine de la santé, visés à l'article 14 du présent projet de loi, et des traitements relevant de l'article 26 de la loi en vigueur. Ces formalités seront remplacées, conformément au Règlement, par l'obligation, pour le responsable, d'effectuer préalablement une analyse d'impact lorsque son traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes et de consulter la Commission le cas échéant. Néanmoins, le Règlement prévoit un certain nombre de marges de manœuvre permettant aux Etats membres de maintenir ou d'établir des formalités préalables à titre de condition ou garantie supplémentaire.

- La Commission souscrit à l'orientation générale retenue de ne pas traduire l'ensemble des marges de manœuvre permises par le Règlement par le maintien de régimes spécifiques d'autorisation dans la loi « Informatique et Libertés ». La suppression des formalités préalables individuelles s'inscrit pleinement dans la logique du Règlement qui tend à responsabiliser les acteurs mettant en œuvre des traitements de données à caractère personnel. Cette suppression doit également être lue à la lumière des nouveaux pouvoirs de la Commission lui permettant de prescrire, d'une part, des mesures techniques et organisationnelles pour le traitement des données biométriques, génétiques et de santé – à l'exception des traitements mis en œuvre par l'Etat agissant dans l'exercice de ses prérogatives de puissance publique – en vue d'assurer la sécurité des systèmes et, d'autre part, des garanties complémentaires en matière de traitement de données relatives à des infractions.

- Au regard de cette logique générale, la Commission s'interroge toutefois sur le maintien des régimes d'autorisation prévus par des textes spécifiques, tels que, par exemple, les articles L. 581-9 du code de l'environnement, L. 4123-9-1 du code de la défense, R. 162-1-10 du code de la sécurité sociale ou L. 252-1 du code de la sécurité intérieure.

- A l'inverse, elle estimerait utile, comme le permet le Règlement (article 9.4), le maintien du régime d'autorisation préalable des traitements portant sur des données génétiques dans les conditions prévues actuellement par l'article 25–I-2° de la loi. En effet, la sensibilité particulière de ces données, en ce qu'elles peuvent révéler des renseignements sur l'état de santé de la personne auxquelles elles se rapportent mais aussi des membres de sa famille, et les perspectives de développement d'offres commerciales portant sur de telles données devraient conduire à ce que la Commission soit en mesure d'encadrer préalablement la mise en œuvre de tels traitements.

- Concernant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR), le projet de loi semble postuler un principe général d'interdiction du traitement de cette donnée. Si cette interdiction, à supposer qu'elle corresponde à l'intention du Gouvernement, gagnerait à être explicitée, il est prévu que seul un décret en Conseil d'Etat, pris après avis motivé et publié de la CNIL, peut autoriser son utilisation par des organismes déterminés et pour des finalités limitativement énumérées. Trois catégories de traitements (traitements à finalité exclusivement statistique, traitements répondant à une alerte sanitaire et téléservices de l'administration électronique) seraient quant à elles dispensées d'une telle autorisation par décret.

La Commission souligne l'effort de simplification concernant l'utilisation du NIR dont le régime juridique était devenu, au fil des ans, largement incompréhensible par les responsables de traitement concernés.

Néanmoins, le système envisagé par le projet de loi, qui ne permet l'utilisation du NIR qu'après autorisation par décret en Conseil d'Etat, n'offre aucune souplesse aux responsables de traitement ne pouvant bénéficier des trois exceptions rappelées ci-dessus. A titre d'exemple, les fournisseurs de solutions de télémédecine qui doivent traiter le NIR des patients à des fins de remboursement ne pourraient le faire qu'après y avoir été autorisés par voie réglementaire, ce qui pourrait freiner le développement de dispositifs innovants, en particulier dans le domaine de la santé. De même, les traitements actuellement créés par arrêté ministériel ou décision de l'organe délibérant

d'un établissement public ou d'une collectivité en vertu du II de l'article 27 de la loi en vigueur, qui portent sur le NIR et sont mis en œuvre par des services ayant pour mission de déterminer les conditions d'ouverture d'un droit, d'établir l'assiette ou de recouvrer des taxes de toute nature, devraient faire l'objet d'un décret en Conseil d'Etat.

La Commission estime donc nécessaire de compléter le dispositif prévu en réintroduisant la possibilité de lui permettre d'autoriser l'utilisation du NIR au vu des éléments présentés par le demandeur. Cet ajout semble, de plus, indispensable afin de garantir la sécurité juridique des traitements ayant été préalablement autorisés par la CNIL ou le pouvoir réglementaire à utiliser le NIR.

A défaut, l'objectif de souplesse et de sécurisation des traitements existants ne pourrait être atteint qu'au bénéfice d'un renversement de la logique sous-tendant le projet, en renonçant à un principe d'interdiction et en prévoyant un trépied constitué des autorisations par la CNIL ou par acte réglementaire, des décrets-cadres et d'un certain nombre de dispenses de toute formalité dans les trois cas mentionnés ci-dessus.

- En tout état de cause, le maintien d'un pouvoir d'autorisation de la Commission – que celui-ci soit ou non étendu comme elle le souhaite en matière de traitements portant sur les données génétiques et sur le NIR – doit s'accompagner du maintien du mécanisme des « autorisations uniques », actuellement prévu au II de l'article 25 de la loi du 6 janvier 1978.

- Enfin, la Commission prend acte du maintien de l'autorisation par décret en Conseil d'Etat, pris après son avis motivé et publié, des traitements mis en œuvre pour le compte de l'Etat portant sur des données biométriques nécessaires à l'authentification ou au contrôle des personnes. Elle relève que ce régime d'autorisation sera dorénavant limité aux seuls traitements mis en œuvre par l'Etat « *agissant dans l'exercice de ses prérogatives de puissance publique* » et qui méritent en effet, comme par exemple le fichier TES, une attention particulière.

CHAPITRE III

OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENTS ET SOUS-TRAITANTS

Articles 10 et 22 (Délégué à la protection des données)

A titre liminaire, la Commission relève que le délégué à la protection des données est abordé dans deux articles du projet de loi, qu'elle entend examiner ensemble : à l'article 10 (article 23 nouveau de la loi du 6 janvier 1978 modifiée) qui figure dans le titre premier, commun au Règlement et à la Directive, mais également à l'article 22 (article 70-15 nouveau de la même loi) qui est propre à la Directive.

Sur l'article 10 du projet de loi (article 23 nouveau de la loi du 6 janvier 1978)

L'article 10 du projet de loi vise à introduire la fonction de délégué à la protection des données. En faisant référence dans le premier alinéa de l'article 23 nouveau de la loi du 6 janvier 1978 aux dispositions de la section 4 du chapitre IV du Règlement, le projet de loi reprend les conditions de désignation et d'exercice des missions du délégué telles que prévues par le Règlement et ne prévoit pas de cas de désignation obligatoire

supplémentaires. La Commission souscrit à l'orientation générale de cet alinéa qui fait référence aux dispositions du Règlement et garantit ainsi une bonne lisibilité des obligations sur ce point. Elle appelle cependant l'attention sur les points suivants.

- Au deuxième alinéa de l'article 23 nouveau, sont reprises inchangées les dispositions actuelles relatives à l'information des instances représentatives du personnel de la désignation du correspondant. Or cette information, dont l'opportunité n'est pas contestable, n'est pas prévue par le Règlement, qui ne comporte pas de marge de manœuvre sur ce point, et qui prévoit en tout état de cause une obligation de publication, plus large, des coordonnées du délégué.

- Le troisième alinéa de l'article 23 (nouveau) maintient le principe, initialement consacré par la loi « Informatique et Libertés », de l'interdiction de sanctionner le délégué à raison de l'accomplissement de ses missions. Mais la rédaction de la loi nationale diffère sur plusieurs points de la rédaction du Règlement – à titre d'illustration, la protection est opposable en droit national à « l'employeur », tandis que le Règlement repose sur les notions de responsable de traitement et de sous-traitant, au-delà du seul lien d'employeur à salarié. La coexistence de ces deux niveaux de lecture est de nature à complexifier la compréhension des obligations. Le renvoi au Règlement apparaîtrait dès lors suffisant dans un souci de clarté.

Le projet de loi maintient la possibilité pour le délégué de « *saisir la Cnil en cas de difficultés rencontrées dans l'exercice de ses missions* ». Or le Règlement ne prévoit pas cette faculté, alors qu'il édicte précisément les pouvoirs et missions de ce délégué, qui doivent être harmonisés pour tous les responsables de traitement quelle que soit leur localisation sur le territoire européen. Elle ne semble dès lors pas nécessaire à la Commission, qui rappelle en outre que le Règlement prévoit que le délégué « *coopère avec l'autorité* » et « *fait office de point de contact* », ce qui permettra au délégué de pouvoir contacter la Commission pour toute question.

Enfin, le projet prévoit la possibilité pour le délégué de « *communiquer la liste des traitements effectués à toute personne qui lui en fait la demande* ». Or, d'une part, le projet ne précise pas les conséquences d'un refus de communication tant vis-à-vis du délégué et de son responsable que des personnes qui en font la demande. Cette ambiguïté est de nature à créer une source d'insécurité juridique et à décourager dans ce cadre les désignations volontaires de délégué. D'autre part, si le Règlement permet à chaque responsable de traitement de compléter le socle minimal des missions des délégués, il ne prévoit pas une telle obligation de manière systématique.

Sur l'article 70-15 introduit dans la loi du 6 janvier 1978 par l'article 22 du projet

L'article 70-15 nouveau a pour objet de transposer les dispositions des articles 32, 33 et 34 de la Directive.

- La Commission observe que le projet de loi entend exclure la désignation d'un délégué pour les juridictions dans l'exercice de leur fonction juridictionnelle. L'article 32 de la Directive permet en effet aux Etats membres, de même que le a) du 1 de l'article 37 du Règlement, de prévoir une telle exclusion. Pour autant, la Commission rappelle que les traitements mis en œuvre par les juridictions peuvent relever d'autres domaines que l'exercice de leurs fonctions juridictionnelles (par exemple, pour assurer la sécurité des

locaux ou informatique ou pour la gestion d'activités non juridictionnelles), ce qui induira en tout état de cause une obligation de disposer d'un délégué du fait de leur nature d'organisme public. Par ailleurs, une extension du périmètre de la désignation des délégués, sous réserve de l'adaptation de leurs missions, ne pourrait que contribuer à une meilleure gestion globale des traitements de données à caractère personnel en France.

- S'agissant des missions du délégué à la protection des données telles que prévues à l'article 70-15.I (nouveau) de la loi du 6 janvier 1978, la Commission relève que le projet de loi procède à une transposition incomplète de la Directive, à deux égards.

En premier lieu, les deux premières missions du délégué à la protection des données (information et conseil du responsable de traitement et contrôle du respect des textes visés au 1° et 2° du projet d'article 70-15.III de la loi) ne visent que la présente loi et non pas, comme l'indique la Directive « *d'autres dispositions du droit de l'Union ou du droit des Etats membres en matière de protection des données* » (futur Règlement dit « e-privacy », code du patrimoine, code de la sécurité intérieure, par exemple).

En second lieu, s'agissant de la dernière mission du délégué à la protection des données visée au 5° du projet d'article 70-15. III de la loi, la mission de « *mener des consultations, le cas échéant, sur tout autre sujet* » figurant à l'article 34.e) de la Directive n'a pas été reprise. Il convient donc de l'ajouter.

Articles 11 et 22 (Sous-traitant)

L'article 11 du projet de loi vise à compléter l'article 35 de la loi actuelle en indiquant que le sous-traitant respecte les dispositions prévues par le chapitre IV du Règlement, tandis que l'article 70-7 nouveau inséré dans la loi en vigueur par l'article 22 du projet de loi vise à transposer, sur ce même point, les dispositions de la Directive.

- S'agissant de la modification projetée de l'article 35 de la loi, si le renvoi auquel procède l'article 11 a le mérite de préciser clairement le régime applicable dans le champ du Règlement, la portée du reste de l'article, non modifié, est ambiguë. La Commission renvoie à ses observations générales sur cette problématique plus globale : les autres dispositions n'ont en réalité vocation à s'appliquer qu'aux traitements situés en dehors du champ tant du Règlement que de la Directive, sans que cette vocation soit clairement précisée. Cette ambiguïté devrait être levée.

- S'agissant de l'article 70-7 nouveau de la loi « Informatique et Libertés », qui a pour objet de transposer les dispositions des articles 22 et 23 de la Directive relatifs aux conditions dans lesquelles les responsables de traitement peuvent recourir aux services d'un sous-traitant, la Commission émet deux observations.

S'agissant de la forme, soucieuse de veiller à une bonne intelligibilité du texte et à la bonne compréhension de ces dispositions par les personnes concernées, la Commission est favorable à distinguer clairement les obligations relevant du Règlement de celles relevant de la Directive aux fins d'une meilleure sécurité juridique. D'une manière générale, il serait préférable de reprendre, pour l'ensemble des traitements en dehors du champ du Règlement, la rédaction de l'article 22 de la Directive et de ne pas faire subsister les dispositions actuelles de l'article 35 de la loi de 1978.

S'agissant du fond, la Commission relève que la transposition de l'article 22 de la Directive est globalement satisfaisante. Néanmoins, il conviendrait d'ajouter une référence aux garanties suffisantes que les sous-traitants doivent présenter quant à la mise en œuvre de mesures « organisationnelles » appropriées, et non seulement de mesures « techniques » (article 22.1 de la Directive). De même, elle rappelle que le droit national, qui pourra être complété sur certains de ces points par voie réglementaire, dont il conviendrait de prévoir l'intervention dans le présent projet de loi, devrait prévoir la forme écrite du contrat, qui peut se présenter sous la forme électronique, et reprendre toutes les précisions de l'article 22.3 de la Directive sur le contenu obligatoire du contrat s'agissant, d'une part, des mentions relatives aux paramètres du traitement (objet, durée, nature, finalité, types de données, catégories de personnes, droits et obligations du responsable) et, d'autre part, des mentions exigées par les dispositions du c), du e) et du f) de ce même article 22.3.

CHAPITRE IV DISPOSITIONS RELATIVES A CERTAINES CATEGORIES PARTICULIERES DE TRAITEMENT

Article 12 (Données d'infraction)

L'article 12 du projet de loi vise à modifier les dispositions de l'article 9 de la loi « Informatique et Libertés », relatives au traitement de données portant sur des infractions. L'article 10 du Règlement limite en effet, tout comme les dispositions nationales actuellement en vigueur, les possibilités de traitement de ces données, tout en permettant au droit national d'en autoriser le traitement, sous réserve de garanties appropriées, hors du contrôle de l'autorité publique. Dans ce contexte, deux séries de modifications de l'article 9 sont prévues.

En premier lieu, le projet de loi vise à clarifier le champ d'application de cet article, en prévoyant que ses dispositions s'appliquent aux traitements de données relatives aux « *condamnations pénales, aux infractions ou aux mesures de sécurité connexes* ». Ces précisions, qui constituent la reprise exacte des termes de l'article 10 du Règlement, limitent ainsi expressément le champ d'application de ces dispositions à la seule sphère pénale. Elles n'appellent pas d'observation particulière de la part de la Commission, qui a toujours interprété ces dispositions comme limitées à la matière pénale.

En second lieu, le projet de loi vise à étendre les responsables de traitement autorisés à traiter de telles données à trois nouvelles catégories.

Il s'agit tout d'abord des personnes morales de droit privé collaborant au service public de la justice. La Commission estime opportun l'ajout de cette catégorie de responsables de traitement, dans la mesure où de tels organismes doivent en effet traiter des données d'infractions aux fins du bon exercice de leurs missions, sans pour autant pouvoir être qualifiés de « *personnes morales gérant un service public* », au sens de l'article 9-1° de la loi du 6 janvier 1978.

S'agissant des garanties qui doivent nécessairement encadrer le traitement de ces données, la Commission prend acte que le projet de loi renvoie à un décret en Conseil d'Etat, pris après avis de la Commission, la définition des catégories de personnes morales ainsi habilitées à traiter des données d'infractions. Elle estime néanmoins que l'alinéa projeté pourrait utilement prévoir que ce traitement ne peut avoir lieu que dans la stricte mesure nécessaire à l'exercice de ces missions, afin de limiter les finalités pour lesquelles ces données particulières peuvent être traitées par ces personnes morales.

La deuxième catégorie de responsables de traitements que le projet de loi vise à autoriser à traiter des données relatives aux infractions est constituée des personnes physiques ou morales victimes d'infractions ou mises en cause dans une procédure. Cet ajout vise à donner suite à la décision DC n° 2004-499 du Conseil constitutionnel qui avait censuré pour incompétence négative des dispositions en ce sens, tout en rappelant que cette déclaration d'inconstitutionnalité « *ne saurait être interprété[e] 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* ».

La Commission, qui a pu autoriser certains traitements de données relatives à des infractions mis en œuvre par des victimes d'infractions sur le fondement de cette réserve, accueille dès lors favorablement l'objet de cette disposition centrée sur le droit à agir en justice. Elle relève que des garanties sont prévues afin de limiter les atteintes au droit au respect de la vie privée susceptibles de résulter de tels traitements, et notamment la restriction des finalités pour lesquels ceux-ci pourraient être mis en œuvre, le rappel de la nécessité de ne conserver les données que pour une durée proportionnée à ces finalités et les limitations prévues s'agissant de la communication de telles données aux tiers.

Il est également prévu que les réutilisateurs des décisions de justice mises à disposition du public soient autorisés à traiter des données d'infractions. Les dispositions du code de justice administrative et du code de l'organisation judiciaire imposent en effet la mise à disposition du public, en open data, de l'ensemble des décisions des juridictions administratives et judiciaires (décisions de premier ressort, d'appel et de cassation), dans le respect de la vie privée des personnes concernées et après une analyse du risque de ré-identification des personnes concernées. Un décret en Conseil d'Etat, qui sera pris après avis de la Commission, doit en fixer les modalités d'application. Il est prévu que les données contenues dans ces décisions soient, non pas anonymisées, mais pseudonymisées, conformément à la recommandation de la Commission de 2001.

Dans la mesure où il s'agit donc de données personnelles, offertes à la réutilisation mais dans des conditions conformes au droit à la protection des données, qui peuvent porter sur des infractions ou condamnations, la Commission estime nécessaire d'autoriser par la loi leur traitement par des réutilisateurs, dans des conditions appropriées.

A cet égard, la Commission relève que seuls les réutilisateurs des jugements et décisions mentionnés aux codes précités, c'est-à-dire de données ayant fait l'objet d'une pseudonymisation plus forte que celle appliquée aujourd'hui aux décisions de justice, sont concernés par les dispositions projetées. Ces traitements sont en outre soumis à une condition impérative : n'avoir ni pour objet ni pour effet de permettre la réidentification des personnes concernées. La Commission prend acte que ces dispositions inscrivent ainsi dans la loi ses propres recommandations en matière de réutilisation des décisions de justice.

Elle relève néanmoins que les décisions de justice sont également susceptibles de comporter des données sensibles au sens de l'article 8 de la loi. Elle appelle dès lors l'attention du Gouvernement sur la nécessité de prévoir des dispositions législatives, conformes à celles prévues par le Règlement s'agissant du traitement de ces données, afin d'autoriser la réutilisation des données contenues dans ces décisions. Le traitement des données sensibles devrait en tout état de cause être soumis à la même condition d'interdiction de réidentifier les personnes concernées, sans préjudice d'autres garanties.

Article 13 (Archives, recherche scientifique et statistique)

L'article 13 du projet de loi vise à modifier l'article 36 de la loi du 6 janvier 1978, afin de faire application des dispositions prévues à l'article 89 du Règlement relatives aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique et à des fins statistiques.

Le Règlement prévoit un régime particulier pour ces traitements, qui peuvent bénéficier directement, dans certaines conditions, de dérogations substantielles au cadre général et qui peuvent en outre faire l'objet de dispositions nationales autorisant des dérogations supplémentaires. Le Règlement retient en outre une interprétation large des notions de recherche historique, qui comprend par exemple les recherches à des fins généalogiques, de recherche scientifique, qui couvre notamment le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé, et de fins statistiques, qui ne se réduit pas aux productions du service statistique public.

Le projet de loi vise à exercer les marges de manœuvre nationales autorisées par le Règlement pour ces traitements. Ces dispositions seront également applicables aux traitements relevant de la Directive et ne relevant pas du champ du droit de l'Union.

Elles appellent deux séries d'observations de la part de la Commission.

- En premier lieu, sur la rédaction projetée, le projet de loi, qui vise à reformuler les dispositions en vigueur relatives à la possibilité de conserver, aux fins de tels traitements, les données à caractère personnel au-delà de la durée de conservation initialement fixée, fait référence à la durée prévue au e) du 1 de l'article 5 du Règlement. Si cette possibilité est expressément prévue par ces dispositions et n'est donc pas nécessaire en droit national s'agissant des traitements relevant du champ d'application du Règlement, ces dispositions ne sont en revanche pas applicables aux autres traitements soumis à la loi du 6 janvier 1978. La Commission estime dès lors nécessaire de clarifier la rédaction de ces dispositions pour en afficher clairement la vocation horizontale.

- En second lieu, sur le fond, la Commission relève que le projet de loi vise à faire application de l'ensemble des dérogations autorisées par le Règlement, sur les droits des personnes ou sur les obligations des responsables de traitement.

Néanmoins, si le projet de loi renvoie aux garanties que le Règlement impose en tout état de cause, la Commission relève que ces dispositions recouvrent un ensemble très

hétérogène de traitements de données et ont vocation à concerner des catégories de responsables de traitement particulièrement variées.

De même, le projet de loi ne prévoit aucune distinction entre les catégories de finalités prévues, alors même que les conditions de traitement des données peuvent et doivent être précisément adaptées à chacune de ces catégories, par exemple en termes de pseudonymisation ou d'exercice des droits des personnes. Il ne prévoit pas davantage de distinction entre les objectifs généraux poursuivis par ces traitements, à l'exception des traitements archivistiques, et notamment entre ceux qui sont mis en œuvre à des fins d'intérêt public et ceux qui poursuivent un intérêt privé ou un intérêt commercial.

La Commission estime que ces distinctions, en particulier la justification éventuelle d'un intérêt public, pourraient être prises en compte au niveau législatif pour encadrer davantage l'intervention du pouvoir réglementaire, afin de moduler, le cas échéant, l'étendue des dérogations possibles et les garanties associées à chaque catégorie de traitements, afin de s'assurer que les dispositions projetées comportent les garanties légales propres à permettre une conciliation entre la protection des données personnelles et les intérêts poursuivis.

S'agissant de ces garanties, il est prévu, outre la mise en œuvre des mesures techniques et organisationnelles mentionnées à l'article 89 du Règlement, qu'un décret en Conseil d'Etat pris après avis de la Commission définisse les conditions et garanties appropriées pour les traitements mis en œuvre à des fins de recherche scientifique ou historique et à des fins statistiques. Des garanties supplémentaires et adaptées à chaque catégorie de traitement, portant par exemple sur les modalités d'exercice des droits des personnes ou des conditions d'accès aux données, sont en effet nécessaires pour assurer une protection suffisante des données personnelles.

La Commission estime dès lors que le projet de loi devrait prévoir les éléments que doit comporter ce décret d'application, et notamment les objets de ces garanties et l'adaptation de l'étendue des dérogations précitées en fonction des catégories concernées de traitement et d'intérêt poursuivi.

Elle considère en outre qu'un tel décret d'application devrait également être prévu s'agissant des traitements mis en œuvre à des fins archivistiques dans l'intérêt public, dont les conditions exactes de mise en œuvre ne sauraient être déterminées uniquement par les dispositions applicables en matière d'archives publiques. Ce décret pourrait en particulier prévoir les modalités d'exercice des droits des personnes concernées par ces traitements ainsi que les limitations afférentes aux modalités de diffusion des données traitées, en matière d'indexation sur les moteurs de recherche externe par exemple.

Enfin, la Commission rappelle qu'elle dispose d'un pouvoir de certification et d'homologation de processus d'anonymisation des données, en vertu de l'article 11-2°-g) de la loi du 6 janvier 1978, et d'une solide expertise des processus de pseudonymisation, qui constituent une des garanties prévues pour l'ensemble de ces traitements par le Règlement. Elle estimerait dès lors utile de compléter ces dispositions et de mentionner expressément la possibilité de certifier ou homologuer des processus de pseudonymisation dans le cadre des traitements relevant de l'article 36 de la loi précitée, tel que modifié par le présent projet de loi.

Article 14 (Chapitre IX données de santé)

L'article 14 du projet de loi vise à insérer dans l'actuel chapitre IX de la loi l'ensemble des dispositions relatives aux traitements de données à caractère personnel dans le domaine de la santé ; il comporte à cette fin deux sections : l'une relative aux dispositions générales, l'autre relative aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

A titre liminaire, la Commission estime utile qu'un chapitre de la loi soit dédié aux traitements de données de santé. Elle prend acte de l'économie générale retenue qui ne vise pas à bouleverser les principes en matière de traitement de données de santé qui, pour ceux issus de la loi de modernisation de notre système de santé de janvier 2016, rentrent seulement en application depuis quelques mois. Elle relève toutefois le maintien d'un processus d'autorisation exigeant, encadrant les traitements relatifs à la recherche dans le domaine de la santé, en comparaison de l'allègement général des formalités préalables portées par le Règlement et le projet de loi qui lui est soumis.

En tout état de cause, la Commission s'interroge très fortement sur la rédaction de ce chapitre qui opère une confusion entre les règles applicables, d'une part, aux traitements à des fins de recherche, d'étude et d'évaluation et, d'autre part, celles – nécessairement plus générales - applicables aux autres traitements comportant des données de santé. Il en résulte une réelle incertitude juridique, notamment sur les outils de simplification développés précédemment par la Commission en la matière.

- Plus précisément, la section 1 relative aux dispositions générales fixe les règles s'appliquant à l'ensemble des traitements de données de santé.

Le projet de loi reprend le dispositif actuellement prévu par la loi « Informatique et Libertés », c'est-à-dire la possibilité de traiter des données de santé en dehors des exceptions limitativement énumérés à l'article 8 de la loi, pour une seule finalité « d'intérêt public » et sous réserve d'une autorisation de la Commission.

Etrangement, le projet énonce ensuite toute une série de dispositions directement reprises de l'actuel chapitre IX : d'une part, des mesures destinées à alléger la procédure d'autorisation (« *méthodologies de référence* », « *jeux de données pouvant faire l'objet d'une mise à disposition* » ou encore « *décisions uniques* »), d'autre part, des règles de fond (interdiction de « *communication* » des données, possibilité pour les professionnels de « *transmettre* » les données à caractère personnel qu'ils détiennent, condition de présentation « *des résultats* », etc.).

Manifestement, ces dispositions n'ont pas vocation à s'appliquer aux traitements comportant des données de santé en dehors de la recherche tels que les vigilances (pharmacovigilance, matériovigilance, cosmétovigilance, etc.), les mécanismes de surveillance sanitaire ou encore les entrepôts de données.

La Commission propose donc de réintégrer l'ensemble des dispositions relatives aux traitements de recherche, d'étude ou d'évaluation dans la section 2, y compris le rôle de l'Institut national des données de santé et ce, tant au regard de ses missions, telles que prévues par le code de la santé publique, que de sa composition.

Ne devraient ainsi plus figurer dans la section 1 que le principe général d'autorisation par la Commission des traitements présentant une finalité d'intérêt public et la faculté, pour elle, d'établir des autorisations uniques sur le modèle de ce qu'elle a déjà pu adopter.

La Commission souligne que ce dispositif, équivalent à celui instauré depuis 2004, a permis un encadrement solide et efficace des traitements de données de santé et a vocation à être complété par les nouveaux pouvoirs dont le projet de loi envisage de doter la Commission (établissement et publication de lignes directrices, de recommandations, de référentiels et de règlements types).

- Dans cette logique, la section 2 relative aux dispositions particulières aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé devrait reprendre, pour l'essentiel, les dispositions actuellement en vigueur au sein du chapitre IX.

Sous cette réserve, les modifications envisagées par le projet de loi aux traitements à des fins de recherche, d'étude ou d'évaluation appellent les principales observations suivantes.

En premier lieu, le projet de loi prévoit que la demande d'autorisation est réputée acceptée lorsque la Commission ne s'est pas prononcée dans un délai de deux mois si l'avis du comité d'expertise compétent est expressément favorable. Ce renversement du principe en vigueur (en cas de silence, la demande est actuellement réputée rejetée) n'est pas sans incidence sur la capacité d'analyse de la Commission au vu du nombre de dossiers qui lui est soumis (plus de 700 demandes d'autorisation reçues en 2017) et, surtout, de leur sensibilité.

Ce principe appelle donc des réserves de la part de la Commission.

En deuxième lieu, le projet de loi maintient une information individuelle atténuée des personnes dont les données sont appelées à être traitées à des fins de recherche. La Commission relève que cette modalité d'information n'est pas conforme aux exigences posées par les articles 13 et 14 du Règlement.

En troisième lieu, le projet de loi contient des dispositions en contradiction avec celles du code de la santé publique.

D'une part, il maintient le principe du consentement des personnes concernées dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants. Cette disposition est contraire à celles de l'article L. 1131-1-1 du code de la santé publique. La Commission estime indispensable une coordination entre ces deux dispositions dans le sens d'une protection renforcée des personnes.

D'autre part, les dispositions du projet de loi maintiennent des dérogations à l'information des titulaires de l'autorité parentale incompatibles avec les dispositions du code de la santé publique. En effet, ce dernier ne prévoit que des dérogations à l'obligation de recueillir le consentement de chacun des titulaires de l'autorité parentale et non à celle de les informer.

La Commission estime donc nécessaire d'harmoniser l'ensemble de ces dispositions.

Enfin, la Commission propose de supprimer le projet d'article 62 de la loi, dans la mesure où tout transfert de données à caractère personnel hors Union européenne doit être conforme aux conditions établies par le Règlement, y compris pour les données codées.

CHAPITRE IV DISPOSITIONS PARTICULIÈRES RELATIVES AUX DROITS DES PERSONNES CONCERNÉES

Article 15 (Mineurs)

Cet article dispose, conformément à l'article 8 du Règlement, qu'un mineur, à compter de l'âge de 16 ans, peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information. En dessous de 16 ans en revanche, le consentement parental sera nécessaire pour que le traitement soit licite. Le projet traduit ainsi le choix de ne pas mobiliser la marge de manœuvre prévue par le Règlement, qui autorise les Etats membres à abaisser ce seuil jusqu'à 13 ans.

- A titre liminaire, la Commission est consciente du décalage entre cette disposition et la réalité des pratiques numériques des mineurs.

Pour autant, il lui paraît nécessaire d'articuler la nécessaire prise d'autonomie des jeunes et la protection particulière de leurs données personnelles qui s'impose en cette période de leur vie, l'adolescence, où la divulgation de leurs données et les atteintes potentielles à leur vie privée en résultant peuvent avoir des effets redoutables sur leur avenir.

- A cet égard, au regard de l'ensemble des droits de l'enfant tels que reconnus dans notre législation nationale, la Commission n'a pas identifié d'éléments déterminants justifiant qu'il soit dérogé au seuil fixé par défaut à 16 ans par le Règlement pour le consentement aux services proposés en ligne.

En effet, si les seuils d'âge sont variables en droit interne selon l'objet de chaque législation, le seuil de 16 ans correspond à une frontière reconnue par le droit commun dans de nombreux contextes juridiques, en particulier en matière contractuelle et bancaire, avec une portée variable selon les actes en cause.

- En outre, le recueil du consentement parental prévu par le Règlement, s'agissant des enfants de moins de 16 ans, peut être considéré, en dépit des limites rencontrées dans la pratique, comme un moyen d'instaurer une occasion de dialoguer entre les parents et leurs enfants sur la façon dont ces derniers entendent protéger leurs données personnelles sur internet et sur les précautions à faire valoir auprès d'eux.

- Au demeurant, quel que soit l'âge retenu dans les législations nationales, se pose la question des modalités pratiques d'application. Pour donner toute son effectivité à ces dispositions, il conviendrait de déterminer avec précision, par exemple par des codes de conduite ou des mécanismes de certification, les obligations propres auxquelles

seront tenus les responsables de traitements concernés pour vérifier l'âge des personnes mineures et s'assurer respectivement de leur consentement éclairé comme de celui de leurs parents, et ce par une information spécifique, compréhensible et adaptée et en prenant compte la nature des services offerts.

En particulier, il est indispensable de prévoir des obligations renforcées s'agissant de l'utilisation des données des personnes mineures à des fins de profilage publicitaire.

- Enfin, pour aider les adolescents, les parents et les personnels éducatifs à mieux comprendre et à mesurer les enjeux liés à l'utilisation et à la divulgation des données personnelles, la Commission souligne qu'il est plus que jamais indispensable de développer et de promouvoir une véritable éducation citoyenne au numérique.

Article 16 (Profilage)

L'article 10 de la loi dans sa rédaction actuelle – dont le premier alinéa, relatif aux décisions de justice, n'est pas modifié par le projet de loi – pose en son deuxième alinéa un principe d'interdiction des décisions produisant des effets juridiques « *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* », sous réserve du troisième alinéa – qui exclut de la notion de décision reposant exclusivement sur un traitement automatisé les décisions prises au titre d'un contrat ou sur demande.

- La modification projetée de ces dispositions poursuit tout d'abord un objectif de mise en cohérence entre la loi et l'article 22 du Règlement, qui n'apparaît pas complètement satisfait.

Ainsi, la Commission relève que, en conséquence de la suppression du 3ème alinéa de son article 10, la loi nationale ne mentionne plus les exceptions prévues par le Règlement lui-même dans ces hypothèses (contrat, consentement) moyennant le droit pour les personnes concernées « *d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision* ».

De même, le projet de loi maintient un certain décalage, entre droit national et Règlement, susceptible de générer des difficultés d'interprétation. Le Règlement raisonne en effet en termes de droit individuel à ne pas faire l'objet d'une décision fondée sur un traitement intégralement automatisé, alors que la loi continue à raisonner en termes d'interdiction pour l'auteur de la décision de procéder à un tel traitement. En outre, le Règlement mentionne les traitements automatisés en général, « *y compris le profilage* », tandis que le projet de loi ne couvre, comme l'article 10 de la loi en vigueur, que les traitements destinés à « *prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée* ». Enfin, l'article 22 du Règlement s'applique non seulement aux décisions produisant des effets juridiques, mais aussi à celles affectant la personne « *de manière significative de façon similaire* ».

- La Commission appelle surtout l'attention sur une modification particulièrement problématique de cet article 10. Le projet de loi lève en effet le principe d'interdiction concernant les décisions administratives individuelles prises exclusivement sur la base d'un traitement automatisé.

En premier lieu, la Commission souligne que le projet renverse ainsi, dans le champ particulièrement emblématique que constitue l'action administrative, le principe général et majeur d'intervention humaine systématique dans la prise de décisions à effet juridique. Cette disposition du projet de loi revêt une portée considérable.

En deuxième lieu, la Commission estime que le projet de loi ne garantit pas la présence des « *mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* » qu'impose le Règlement. Le seul renvoi aux possibilités prévues aux articles L. 411-1 et suivants du code des relations entre le public et l'administration (CRPA), à savoir de former un recours administratif contre toute décision administrative, ne saurait, de manière générale, satisfaire à ces exigences européennes. De même, les mesures actuellement prévues par le CRPA et relatives à la transparence des paramètres des traitements algorithmiques mis en œuvre par les administrations ne constituent pas davantage à eux seuls des garanties suffisantes.

Si les garanties exigées par le Règlement peuvent le cas échéant être modulées en fonction de la portée de la décision concernée pour les intérêts des citoyens et si la loi n'a pas nécessairement à prévoir elle-même l'ensemble des garanties, la formulation du projet de loi n'apparaît pas satisfaisante en l'état.

En troisième lieu, la Commission rappelle que l'intervention humaine peut faire l'objet d'aménagements. Elle regrette dès lors que la modification de l'article 10 projetée n'ait pas été précédée d'une analyse d'impact approfondie, portant notamment sur les modalités garantissant une intervention humaine sous la forme, par exemple, d'un contrôle humain garantissant la maîtrise de l'algorithme, ou l'aménagement dans certains cas d'un temps permettant à la personne de présenter des observations avant l'intervention de la décision proprement dite.

Article 17 (Limitation des droits des personnes pour certains traitements de l'Etat)

L'article 17 du projet de loi prévoit de créer un nouvel article 37-1 de la loi du 6 janvier 1978 modifiée, afin de faire application des possibilités ouvertes par l'article 23 du Règlement s'agissant des limitations pouvant être apportées à la portée des droits des personnes concernées et des obligations des responsables de traitement en ce domaine. Ces dispositions permettent au droit national de prévoir de telles limitations, dès lors qu'elles respectent les libertés et droits fondamentaux et constituent une mesure nécessaire et proportionnée pour garantir certains intérêts publics.

Le projet de loi vise à faire application de ces marges de manœuvre, dont la Commission ne conteste aucunement la nécessité, et dispose que l'acte réglementaire portant création d'un traitement mis en œuvre pour le compte de l'Etat et relevant du champ d'application du Règlement peut prévoir de telles limitations, dans les conditions prévues par l'article 23 précité.

Ledit article prévoit que ces limitations doivent être prévues par des mesures de droit national, qui doivent comporter de nombreuses précisions. Si la Commission prend acte que ces dispositions n'imposent pas de prévoir, dans la loi du 6 janvier 1978, l'ensemble de ces précisions, elle relève que le caractère général de la rédaction projetée ne permet pas d'appréhender l'étendue des limitations dont pourraient bénéficier les traitements concernés, la nature exacte de ceux-ci et, par conséquent, le caractère

proportionné des limitations ainsi autorisées par la loi. Elle relève en outre que le projet de loi renvoie au seul pouvoir réglementaire le soin de définir, pour chaque traitement ou pour des catégories de traitements, la portée exacte de ces limitations à l'ensemble des droits des personnes concernées. Ainsi, aucun encadrement général des conditions d'application de ces dérogations substantielles au droit à la protection des données personnelles n'est prévu par le projet de loi et seul un contrôle *a posteriori* et ponctuel de la légalité des limitations effectivement mises en œuvre pourra être exercé.

Par ailleurs, la Commission relève que seuls les traitements mis en œuvre pour le compte de l'Etat sont concernés par les dispositions projetées de l'article 37-1 de la loi «Informatique et Libertés». Ces dispositions excluent donc de leur champ d'application les traitements mis en œuvre par les collectivités territoriales, les établissements publics ou les personnes morales de droit privé ou de droit public gérant un service public, qui pourraient pourtant légitimement bénéficier, dans des conditions appropriées, de certaines de telles limitations. Il en est de même de certains traitements mis en œuvre en application d'une obligation légale, pour lesquels le droit d'opposition, par exemple, peut actuellement être écarté en vertu des dispositions en vigueur de l'article 38 de la loi du 6 janvier 1978.

Au regard de ces éléments, la Commission considère que ces dispositions, qui ne semblent, en l'état de leur rédaction, ni nécessaires ni suffisantes, ne comportent pas les garanties légales de nature à assurer un juste équilibre entre le droit à la protection des données à caractère personnel et les intérêts publics en cause.

CHAPITRE V VOIES DE RECOURS

Article 18 (Action de groupe)

L'article 18 du projet de loi prévoit la possibilité pour la personne concernée de mandater les organismes mentionnés à l'article 43 ter de la loi du 6 janvier 1978, à savoir des associations actives en matière de protection de la vie privée, des associations de défense des consommateurs et des organisations syndicales, aux fins d'exercer en son nom certains droits. Il s'agit du droit d'introduire une réclamation auprès de l'autorité de contrôle et du droit à un recours juridictionnel à l'encontre de l'autorité de contrôle et à l'encontre d'un responsable de traitement ou d'un sous-traitant.

La Commission relève que cette possibilité, directement ouverte par l'article 80 du Règlement s'agissant des associations actives en matière de vie privée, est ainsi étendue à deux nouvelles catégories d'organismes.

Néanmoins, elle relève que l'article 55 de la Directive ouvre les mêmes possibilités, qu'il convient dès lors de prévoir expressément dans le droit national, et que la mention des seuls droits prévus aux articles 77 à 79 du Règlement ne permet pas de s'assurer de la bonne transposition de la Directive sur ce point.

Elle regrette enfin que le projet de loi ne prévoit pas de disposition s'agissant de la possibilité de mandater ces mêmes organismes aux fins d'obtenir réparation du préjudice subi.

Article 19 (Action en justice)

L'article 19 du projet de loi est relatif au pouvoir de la Commission d'ester pour obtenir la saisine de la Cour de Justice de l'Union européenne afin qu'elle apprécie la validité d'un acte de la Commission européenne permettant le transfert de données hors de l'Union européenne. Il prévoit que la Commission peut demander au Conseil d'Etat d'ordonner la suspension ou la cessation du transfert de données, dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, elle estime fondés les griefs avancés, dans l'attente de l'appréciation par la Cour de Justice de la validité d'une décision d'adéquation de la Commission européenne prise sur le fondement du Règlement ou de tout acte pris par la Commission européenne autorisant ou approuvant les garanties appropriées pris sur le fondement du Règlement.

La Commission relève que cette disposition propose une transposition trop étroite, dans la mesure où elle ne vise, d'une part, que les actes de la Commission européenne pris sur le fondement du Règlement alors que la disposition devrait également inclure les actes de la Commission européenne pris sur le fondement des articles de la Directive.

D'autre part, la Commission estime que cette disposition doit être amendée pour permettre également la saisine du Conseil d'Etat en dehors d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, afin que la Commission puisse également agir lorsqu'elle estime que la décision européenne permettant le transfert n'est pas valide. Cette possibilité de saisine d'initiative paraît en outre imposée par l'article 58.5 du Règlement.

TITRE III DISPOSITIONS PORTANT TRANSPOSITION DE LA DIRECTIVE (articles 20, 21, 22 et 28)

Observations générales sur la transposition de la Directive

Sur l'économie générale des articles 20, 21 et 22

L'article 20 du projet de loi prévoit de créer un nouvel article 3bis de la loi du 6 janvier 1978, comportant les définitions prévues dans la Directive qui ne figurent pas dans les dispositions actuellement en vigueur de cette loi.

L'article 21 du projet de loi prévoit pour sa part la suppression des dispositions de l'article 42 de la loi du 6 janvier 1978 relatives à l'exercice indirect des droits des personnes concernées à l'égard des traitements relevant de la Directive, pour lesquels des dispositions spécifiques sont prévues. Ainsi, seuls les traitements mis en œuvre aux fins de contrôle et de recouvrement des impositions pourront être concernés par les dispositions de l'article 42 précité, sous réserve de satisfaire aux conditions prévues à l'article 23 du Règlement s'agissant de limitations aux droits des personnes.

L'article 22 du projet de loi prévoit la création de nouveaux articles 70-1 à 70-25 de la loi du 6 janvier 1978, spécifiquement consacrés aux traitements relevant de la Directive, c'est-à-dire, en substance, aux fichiers de police et de justice qui relèvent actuellement de l'article 26-I-2° de la loi précitée.

Dans l'ensemble, le projet de loi procède à une transposition fidèle de la Directive et apporte dès lors des garanties importantes du point de vue de la protection des données traitées dans ce champ, en ce qui concerne en particulier le délégué à la protection des données, l'obligation de réaliser des analyses d'impact relatives à la protection des données, la notification des violations de données, le principe de *privacy by default*, ou encore les conditions de traitement de certaines données ou de certaines catégories de personnes concernées.

La plupart de ces projets d'articles, qui constituent des reprises intégrales des dispositions de la Directive, n'appellent dès lors pas d'observation particulière de la part de la Commission. Néanmoins, le choix de transposition *a minima* de cet instrument n'emporte pas les mêmes conséquences que celui concernant l'exercice des marges de manœuvre prévues par le Règlement, pour les raisons évoquées dans les observations d'ordre général du présent avis. Les dispositions du projet de loi appellent dès lors les observations suivantes de la part de la Commission.

Sur le champ d'application de ces nouvelles dispositions

La Commission estime que le projet de loi ne permet pas d'appréhender clairement le champ d'application des dispositions projetées.

En effet, le projet d'article 70-1 de la loi du 6 janvier 1978, qui reprend les termes de l'article 1^{er} de la Directive et prévoit que sont soumis à ces nouvelles dispositions, le cas échéant dérogoires aux autres dispositions de la même loi, les traitements mis en œuvre à des fins de prévention et détection d'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* », ne permet pas d'identifier sans équivoque les traitements nationaux relevant de ce champ d'application. En particulier, il ne permet pas d'établir si les traitements « *intéressant la sécurité publique* », au sens des dispositions de l'article 26-I-1° de la loi du 6 janvier 1978, qui ne sont d'ailleurs pas modifiées par le présent projet de loi, relèvent ou non du champ d'application du chapitre XIII (nouveau) de la même loi.

De même, ni l'article 70-1 nouveau ni le projet d'article 70-2 ne permettent de régler la situation des nombreux traitements qui, par les finalités qu'ils poursuivent et les données qu'ils comportent, peuvent relever tout à la fois du champ d'application du Règlement et de celui de la Directive. Il en est ainsi, par exemple, de certains traitements mis en œuvre par l'administration fiscale, en matière d'immigration ou de douanes, qui peuvent avoir notamment pour finalités certaines de celles prévues au projet d'article 70-1 précité. L'imprécision de ces dispositions ne permet pas davantage d'établir le régime juridique applicable aux traitements poursuivant simultanément de telles finalités ainsi que des finalités de sécurité publique et de sûreté de l'Etat.

Au regard de ces éléments, la Commission considère que le projet de loi soulève des problèmes de lisibilité et de sécurité juridique importants, qui peuvent s'avérer

préjudiciables pour les responsables de traitement comme pour les personnes concernées, dont le niveau de protection à l'égard du traitement de leurs données est susceptible de varier de manière substantielle en fonction des règles de droit applicables. Si ces questions de frontières résultent au premier chef de la Directive elle-même et du recours par le législateur européen à deux instruments distincts, la formulation de critères précis permettant de déterminer le ou les régime(s) juridique(s) applicable(s) à ces catégories de traitements devrait être envisagée.

Sur les omissions du projet de loi

Au-delà des dispositions expressément prévues par le projet de loi, la Commission estime que ce projet est incomplet sur certains points, en ce qui concerne notamment la consécration du principe de sécurité du traitement au titre des conditions de licéité du traitement de données, les conséquences qui s'attachent à la qualité de responsable de traitement, la notion de responsabilité conjointe de traitement, les conditions de traitement des données sensibles, l'obligation de faciliter l'exercice des droits des personnes concernées, le principe de protection des données dès la conception ou les conséquences que peut tirer la Commission de la transmission d'une analyse d'impact, dont le contenu n'est d'ailleurs pas davantage précisé, concernant un traitement qu'elle considérerait comme constituant une violation des dispositions de la loi. Si certaines autres dispositions pourraient être transposées par voie réglementaire, la Commission estime dès lors que le projet de loi devrait être complété sur ces points.

Sur le niveau d'ambition du projet de loi

La Commission regrette que le projet de loi ne fasse pas application de la possibilité de prévoir des garanties supérieures en matière de protection des données traitées à des fins pénales, expressément prévue à l'article 1^{er} de la Directive. Si la Commission se félicite du maintien d'une autorisation de mise en œuvre de tels traitements par acte réglementaire pris après son avis publié et motivé, elle relève que le projet de loi n'apporte aucune garantie supérieure à ce que prévoit la Directive, alors que même le droit national et sa pratique ont permis la mise en œuvre de telles garanties, qu'il conviendrait de faire figurer expressément dans ces dispositions spéciales.

Ainsi, le projet de loi comporte de très nombreuses précautions rédactionnelles, qui n'apparaissent ni justifiées ni nécessaires et pourraient donner lieu à un abaissement du niveau de protection des données actuellement assuré au niveau national, en ce qui concerne par exemple la distinction, pourtant fondamentale, entre les données personnelles fondées sur les faits de celles fondées sur des appréciations et entre les différentes catégories de personnes concernées, l'effacement ou la rectification des données et la vérification de leur qualité avant toute transmission ou encore l'identification des personnes consultant, communiquant ou recevant des données.

De manière plus substantielle, le projet de loi ne prévoit aucune disposition concernant le droit d'opposition des personnes concernées, qui doit pouvoir, y compris en ces matières, trouver à s'appliquer dans des circonstances particulières, comme par exemple dans le cadre du traitement de données relatives à des personnes victimes dans le Traitement des Antécédents Judiciaires (TAJ). Il ne prévoit pas davantage de dispositions relatives à l'exercice des droits des personnes par voie électronique, actuellement exclu par les dispositions de l'article 43 bis de la loi du 6 janvier 1978, au traitement de données relatives à des mineurs, qui doit faire l'objet de garanties

particulières dans ses conditions de mise en œuvre, ou aux conditions de traitement des données qui doivent compléter les distinctions prévues au projet d'article 70-9 (nouveau) de la même loi concernant les catégories de personnes concernées.

Comme cela a été rappelé, ce manque d'ambition se révèle tout particulièrement pour les traitements ne relevant pas du champ du droit de l'Union et en particulier pour les traitements intéressant la sûreté de l'État, pour lesquels le projet de loi ne prévoit aucune modification du cadre juridique actuel.

Observations particulières sur la transposition de la Directive

Sur le registre (article 70.11 nouveau de la loi)

Le projet d'article 70-11 de la loi du 6 janvier 1978 a pour objet de transposer les dispositions de l'article 24 de la Directive relatif au registre des activités de traitement des responsables du traitement et des sous-traitants. L'article 24.1 de la Directive impose que les Etats membres prévoient que les responsables du traitement tiennent un registre de toutes les « *catégories d'activités de traitement* » et fixe le contenu de ce registre. L'article 24.2 de la Directive impose que les Etats membres prévoient que chaque sous-traitant tienne un registre de toutes les « *catégories d'activités de traitement* » et fixe le contenu de ce registre. La transposition de ces dispositions constitue un progrès notable en matière de protection des données traitées à des fins répressives.

La Commission s'interroge néanmoins sur la nécessité d'un renvoi à un décret en Conseil d'Etat pour préciser le contenu de ce registre, alors même que l'article 24 de la Directive énumère explicitement les informations devant y figurer. Il conviendrait donc de reprendre dans le projet de loi les informations devant figurer dans le registre du responsable du traitement (article 24.1 de la Directive) et dans le registre du sous-traitant (article 24.2 de la Directive).

Enfin, l'article 24.3 de la Directive prévoit que les registres « *se présentent sous une forme écrite, y compris la forme électronique* ». Cette précision utile n'a pas été reprise dans le projet de loi, qui pourrait compléter l'article 70-11 nouveau sur ce point.

Les violations de données (nouvel article 70-14)

Le projet d'article 70-14 de la loi du 6 janvier 1978 prévoit la notification des violations de données à caractère personnel, auprès de la Commission et des personnes concernées, dans certaines conditions. Cette obligation constitue une avancée majeure de la Directive du point de vue de la protection des données, que le présent projet de loi vise donc à établir dans le droit national.

Les délais de notification à la Commission de telles violations ne sont néanmoins pas prévus, en contrariété avec les dispositions de l'article 30 de la Directive, de même que ceux afférant à leur notification aux personnes concernées. La Commission demande donc que des conditions précises de notification soient prévues, d'autant plus nécessaires que ces conditions ont vocation à être également applicables aux sous-traitants qui doivent notifier les mêmes violations auprès des responsables de traitement.

Elle relève en outre que le projet de loi ne prévoit pas une obligation, mais une simple possibilité, de procéder à une communication publique ou à une mesure similaire quant à l'intervention d'une violation lorsque sa communication aux personnes concernées exige des efforts disproportionnés, contrairement aux dispositions prévues à l'article 31 de la Directive.

Les dispositions prévues au III du projet d'article 70-14 de la loi prévoient, conformément à l'article 31 de la Directive, la possibilité pour la Commission de mettre en demeure le responsable de traitement d'informer les personnes concernées par une violation. La Commission relève que les dispositions générales de la loi « Informatique et Libertés », telles que modifiées par le présent projet de loi, lui confèrent déjà cette prérogative et estime dès lors nécessaire, afin d'asseoir la sécurité juridique de ses actions, de supprimer ces dispositions spécifiques, dont il est prévu au projet d'article 70-1 de la même loi qu'elles s'exercent le cas échéant par dérogation aux dispositions générales.

Cette suppression lui apparaît d'autant plus souhaitable que le IV du même projet d'article 70-14 prévoit la possibilité, pour le responsable de traitement, de retarder, limiter ou ne pas délivrer les informations relatives à la violation aux personnes concernées, si ces informations sont de nature à mettre en danger ou à faire obstacle à certains intérêts publics importants. Si cette possibilité, expressément prévue par la Directive, n'appelle pas de réserve de principe de la part de la Commission, il convient néanmoins de s'assurer que le contrôle de celle-ci sur la légalité d'une absence de communication d'une violation de données aux personnes concernées, qui peut conduire, le cas échéant, à la mise en demeure d'informer ces dernières, comprend nécessairement la vérification du respect de ces conditions, ce que ne permet pas d'établir clairement le projet de loi.

La Commission relève en outre que les dispositions projetées sur ces limitations sont insuffisamment précises par rapport aux dispositions de la Directive, qui prévoient que de telles limitations ne peuvent intervenir que « *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* ». Elle souligne à cet égard que ces dispositions imposent au responsable de traitement un contrôle spécifique à chaque situation et ne sauraient être interprétées comme autorisant de telles limitations pour l'ensemble des violations affectant un traitement ou des catégories de traitements.

Enfin, la Commission estime que le projet d'article 70-14 devrait être complété de dispositions réglementaires d'application, qui devraient être expressément prévues par le projet de loi, afin de fixer des modalités de mise en œuvre de ces nouvelles obligations conformes aux dispositions des articles 30 et 31 de la Directive. En particulier, le contenu des notifications adressées à la Commission, le contenu des notifications aux personnes concernées, ainsi que les procédures exactes de ces notifications devraient être définis par décret en Conseil d'Etat pris après avis de la Commission.

Sur les droits des personnes (articles 70-16 à 70-20)

Le projet d'article 70-16 de la loi « Informatique et Libertés » instaure un droit à l'information des personnes qui était, jusqu'à présent exclu pour les traitements ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales. La Commission relève qu'il s'agit d'une avancée importante pour les droits des personnes mais souligne néanmoins que son manque de précision peut en restreindre la portée.

Conformément à la Directive, une distinction est en effet opérée entre, d'une part, les informations qui doivent être systématiquement mises à disposition des personnes et, d'autre part, les informations fournies de manière additionnelle et « *dans des cas particuliers* », sans que ces cas soient pour autant précisés. La Commission souligne que cette simple reprise des termes de l'article 13 de la Directive ne permet pas de déterminer les situations dans lesquelles les personnes sont en droit d'obtenir de telles informations complémentaires de la part du responsable du traitement. Cette absence de lisibilité peut être un frein à l'exercice des droits tout en étant source d'insécurité juridique pour les responsables des traitements concernés.

La Commission estime dès lors, au regard de la nature de ces informations additionnelles, qui peuvent notamment figurer dans l'acte réglementaire portant création du traitement en cause, que les cas dans lesquels elles devraient être fournies à la demande de la personne concernée ne devraient pas être excessivement limités et pourraient en particulier comprendre les hypothèses de collecte directe des données auprès de ces personnes.

Elle estime que cette clarification est en outre rendue nécessaire pour lui permettre d'exercer pleinement la compétence nouvelle qui lui est confiée, en vertu du projet d'article 70-20 de la loi du 6 janvier 1978, à savoir l'exercice « indirect » de ce droit à l'information additionnelle en cas de restriction du responsable de traitement.

A cet égard, la Commission observe que la portée de ce droit est ambiguë, dans la mesure où son exercice viserait à fournir ou non des informations générales sur la base de demandes individuelles, sous le contrôle de la Commission. En tout état de cause, le projet de loi ne permet pas d'écarter clairement des restrictions au cas par cas de ce droit à l'information, sur la base de la seule appréciation du responsable de traitement. Afin d'éviter toute incertitude juridique, la Commission estime que les situations dans lesquelles la fourniture d'informations peut être retardée, limitée ou refusée et pour lesquelles un tel droit « indirect » peut dès lors s'appliquer devraient être prévues à titre général par l'acte réglementaire portant création du traitement en cause.

Le projet d'article 70-17 de la loi précitée définit le droit d'accès applicable aux traitements relevant du champ de la Directive en posant le principe d'un droit d'accès direct des personnes auprès du responsable du traitement, afin d'obtenir la confirmation que des données à caractère personnel la concernant sont ou non traitées et, dans ce dernier cas, la communication des données. La personne est également en droit d'obtenir, dans le cadre de ce droit d'accès, d'autres informations limitativement énumérées telles que les finalités du traitement, les catégories de données à caractère personnel concernées.

La Commission souligne que cet article omet néanmoins le droit pour la personne de se faire communiquer les informations disponibles quant à l'origine des données, qui

constitue une information importante, notamment en cas de donnée inexacte, incomplète ou périmée, et expressément prévue par l'article 14 de la Directive.

Le projet d'article 70-18 de la loi du 6 janvier 1978 prévoit que la personne concernée doit être informée par le responsable du traitement de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs de ce refus.

La Commission relève que ces dispositions ne distinguent pas clairement les droits de rectification et d'effacement ouverts aux personnes concernées et ne créent pas à leur profit un droit autonome à la limitation du traitement, pourtant rendu possible par les dispositions de la Directive. La Commission estime que ce projet d'article devrait dès lors être complété et précisé sur ces points.

Le projet d'article 70-19 de la même loi a pour objet de transposer l'article 17 de la Directive qui prévoit l'exercice des droits de la personne concernée par l'intermédiaire de l'autorité de contrôle en cas de restriction de ses droits. De telles restrictions doivent être définies par l'acte réglementaire portant création du traitement en cause.

Le projet de loi ne prévoit la possibilité de saisir la Commission en matière de rectification ou d'effacement des données que dans le cas où la personne ne peut obtenir de la part du responsable du traitement l'information quant à sa décision de refus et ses motifs. La Commission rappelle que, dans cette hypothèse, son intervention dans les conditions prévues par l'article 41 de la loi du 6 janvier 1978 modifiée peut permettre de rectifier ou d'effacer des données et ne saurait se limiter à la seule vérification des motifs du refus du responsable du traitement. Il en est naturellement de même en matière de communication des informations demandées par les personnes concernées.

La Commission suggère enfin de modifier la rédaction du IV du projet d'article 70-19 de la loi, afin de définir plus précisément le périmètre de l'exercice indirect des droits de la personne, dans les termes suivants : « En cas de restriction des droits de la personne concernée intervenue en application du II ou du III de l'article 70-19 ».

Le projet d'article 70-20 de la même loi rappelle la possibilité pour les personnes concernées de saisir la Commission en cas de restriction des droits et fixe le cadre d'intervention de la celle-ci, à savoir les deuxième et troisième alinéas de l'article 41 de la loi en vigueur.

La Commission relève que, pour ce qui concerne l'accès, ces dispositions permettent uniquement aux personnes d'obtenir, sous réserve de l'accord du responsable du traitement, l'accès aux données les concernant « contenues » dans le traitement, ce qui est plus restreint que les exigences créées par le projet d'article 70-17 de la loi et conformes aux dispositions de la Directive. Elle souligne que les responsables de traitement devront donc être mesure de mettre l'ensemble de ces informations, et notamment les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, à la disposition du membre de la Commission qui sera chargé des vérifications au titre de l'article précité. De même, la rédaction de l'article 41 devrait être complétée des nouveaux droits créés par le présent projet de loi.

Enfin, le projet prévoit que, lorsque la Commission informe la personne qu'il a été procédé aux vérifications nécessaires, elle doit également lui indiquer son droit de former un recours juridictionnel. La Commission relève que les vérifications menées au titre de l'article 41 par un membre de la Commission peuvent conduire, en accord avec le responsable du traitement, à lever les restrictions initiales tant pour l'information, l'accès ou la rectification et qu'il lui semble donc nécessaire de préciser la rédaction projetée, en mentionnant par exemple « lorsque la Commission informe uniquement la personne concernée qu'il a été procédé aux vérifications nécessaires ».

Sur les transferts de données (articles 70-23 à 70-25)

Les projets d'articles 70-23 à 70-25 de la loi du 6 janvier 1978 concernent les règles applicables 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 européenne. L'article 70-23 (nouveau) vise à transposer les dispositions de la Directive relatives aux principes généraux applicables aux transferts de données à caractère personnel. Les dispositions prévues au 2° dudit article transposent le principe suivant lequel les données à caractère personnel ne peuvent être transférées qu'à un responsable dans un pays tiers ou à une organisation internationale qui est une autorité compétente chargée dans cet Etat des fins visées au paragraphe 1 de l'article 1^{er} de la Directive. La Commission estime que ce projet d'article ne transpose pas correctement le texte de la Directive, dans la mesure où le projet de loi ne fait référence qu'aux fins relevant en France du 1° de l'article 70-1, sans viser les autres Etats membres, ce qui restreint le champ de cette disposition.

De même, elle considère que les dispositions prévues au 4° du même projet d'article 70-23 ne sont pas conformes aux dispositions correspondantes de la Directive. En effet, les conditions permettant de procéder à un transfert de données y sont présentées comme potentiellement alternatives et cumulatives, alors que l'article 35 de la Directive établit clairement une hiérarchie au sein de ces conditions.

Sur la traçabilité (70-12) et les dispositions transitoires de l'article 28 du projet de loi

Les dispositions prévues au projet d'article 70-12 de la loi « Informatique et Libertés » concernant les mesures de traçabilité des opérations de traitement que doit mettre en œuvre tout responsable de traitement n'appellent pas d'observations particulières de la part de la Commission. Celle-ci observe néanmoins que l'article 28 du projet de loi prévoit, conformément à l'article 63 de la Directive et dans certaines conditions, une entrée en vigueur de ces obligations à une date ultérieure, ne pouvant excéder le 6 mai 2026.

Si la Commission est consciente des contraintes liées à ces nouvelles obligations, elle rappelle que les traitements relevant actuellement de l'article 26 de la loi « Informatique et Libertés » prévoient déjà, dans leur majorité, des mesures rigoureuses de traçabilité et qu'une journalisation minimale pourrait être prévue pour les traitements qui ne permettent pas de satisfaire à l'ensemble des conditions posées au projet d'article 70-12 de la même loi. Dans ces conditions, elle estime que les motifs de ces reports, qui doivent être notifiés à la Commission européenne, devraient également lui être communiqués et que l'acte réglementaire déterminant les traitements concernés par ces reports devrait faire l'objet d'un contrôle préalable de la Commission, afin de s'assurer que ces dérogations temporaires à une exigence

impérieuse en matière de protection des données soient effectivement limitées aux cas strictement nécessaires.

TITRE IV **HABILITATION A AMELIORER L'INTELLIGIBILITE DE LA LEGISLATION APPLICABLE A LA PROTECTION DES DONNEES**

Article 23 (Habilitation)

La Commission insiste sur la nécessité d'anticiper l'adoption de l'ordonnance afin d'assurer une lisibilité satisfaisante du droit français de la protection des données à caractère personnel.

TITRE V **DISPOSITIONS FINALES**

Articles 24 et 25 (Liste dite « de l'article 31 »)

La Commission relève que le projet de loi laisse à la charge des responsables de traitement une obligation déclarative en cas de modification ou de suppression d'un traitement déclaré avant le 25 mai 2018.

Conformément aux objectifs de simplification définis par le Règlement, la Commission demande l'adaptation de l'article 24 (4°) du projet de loi afin de limiter aux seules formalités qui perdurent après le 25 mai 2018 l'application des dispositions de l'article 30-II de la loi « Informatique et Libertés ».

Pour marquer la mise en œuvre d'un régime nouveau de formalités préalables auprès de la Commission et préserver la transparence relative aux formalités reçues, les articles 24 (5°) et 25 du projet de loi organisent :

- la mise à disposition durant dix ans d'une « liste article 31 » figée au 24 mai 2018 (ancien régime des formalités) ;
- le maintien du principe d'une « liste article 31 », qui ne recenserait plus que les formalités réalisées à compter du 25 mai 2018.

Dans un souci de coordination avec l'article 25 du projet de loi (dont les dispositions transitoires n'ont pas vocation à être inscrites dans l'article 31 de la loi du 6 janvier 1978) et d'intelligibilité, la Commission estime souhaitable qu'une précision soit apportée dans l'article 24 (5°) sur le fait que seuls les traitements ayant fait l'objet d'une formalité auprès de la Commission à compter de l'entrée en vigueur de la nouvelle loi sont concernés par cette « liste article 31 » renouvelée.

La Commission propose également de viser dans cet article, outre les formalités prévues par les articles 26 et 27, celles prévues au chapitre IX de la loi pour une mise à disposition d'une liste exhaustive des formalités accomplies auprès de la Commission. Enfin, elle estime souhaitable d'adapter le contenu de cette liste pour l'actualiser et la rendre plus intelligible, en supprimant notamment les mentions relatives à la date de

la déclaration du traitement, à la dénomination du traitement, à la fonction de la personne auprès de laquelle s'exerce le droit d'accès et aux destinataires (la mention des seules catégories de destinataires étant suffisante).

Article 26 (Traitement des antécédents judiciaires)

L'article 26 du projet de loi prévoit de modifier l'article 230-8 du code de procédure pénale (CPP), relatif aux traitements d'antécédents judiciaires (TAJ) que peuvent mettre en œuvre les services de la police nationale et de la gendarmerie nationale, en application de l'article 230-6 du même code, pour faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Le projet modifie plus précisément les conditions dans lesquelles les personnes mises en cause dans une procédure pénale peuvent demander au procureur de la République territorialement compétent l'effacement anticipé des données à caractère personnel les concernant, pour tirer les conséquences de la décision n° 2017-670 QPC du Conseil constitutionnel en date du 27 octobre 2017.

Par cette décision, le Conseil constitutionnel a en effet jugé que les dispositions du premier alinéa de l'article 230-8 précité portent une atteinte disproportionnée au droit au respect de la vie privée dans la mesure où elles privent les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquiescement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le TAJ. Le projet de loi prévoit dès lors d'étendre la possibilité de demander l'effacement anticipé des données à caractère personnel enregistrées dans le TAJ à l'ensemble des personnes mises en cause dans une procédure pénale, y compris celles ayant fait l'objet d'une condamnation.

La Commission se félicite d'une telle évolution, qui marque un renforcement des droits des intéressés et doit permettre de mieux prévenir le risque d'une conservation excessive des données à caractère personnel.

En ce qui concerne les modalités d'exercice de la faculté nouvelle reconnue aux personnes ayant fait l'objet d'une condamnation, il est prévu qu'en cas de condamnation avec dispense de peine ou dispense de mention au bulletin n° 2 de leur casier judiciaire, la demande adressée au procureur de la République pourra être formée sans délai à la suite de la décision devenue définitive, comme le permet actuellement l'article 230-8 du CPP pour les personnes ayant bénéficié d'une relaxe, d'un acquiescement, d'un non-lieu ou d'une décision de classement sans suite. Dans les autres cas, le projet prévoit que « *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* ».

La Commission prend acte de la nécessité de définir des conditions de recevabilité spécifiques pour les personnes ayant fait l'objet d'une condamnation mais n'ayant bénéficié ni d'une dispense de peine ni d'une dispense de mention au bulletin n° 2 du casier judiciaire.

Elle souligne néanmoins que le critère de recevabilité des demandes d'effacement prévu par le projet de loi semble exiger l'absence de toute mention dans le bulletin n°2 du casier judiciaire, alors que seule la prise en compte de l'absence de mention relative

à la condamnation conduisant l'intéressé à former une demande d'effacement de données dans le TAJ lui apparaît justifiée.

En outre, la nouvelle rédaction du premier alinéa de l'article 230-8 prévue par le projet de loi prévoit expressément que le procureur de la République territorialement compétent peut, d'office ou à la demande de la personne concernée, demander que des données soient effacées, complétées ou rectifiées ou qu'elles fassent l'objet d'une mention, étant rappelé qu'en application du deuxième alinéa de l'article 230-9 du CPP, le magistrat chargé de suivre la mise en œuvre et la mise à jour du TAJ « *dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles* » dans le traitement. Si les prérogatives ainsi mentionnées ne sont pas nouvelles, la Commission estime appropriée la clarification opérée, compte tenu des modifications successives dont l'article 230-8 du CPP a fait l'objet et de la nécessité d'en sécuriser l'interprétation pour la protection des droits des personnes concernées.

Enfin, le projet de loi fixe à deux mois le délai dont dispose le procureur de la République pour se prononcer sur les suites à donner aux demandes dont il est saisi, alors que ce délai est actuellement d'un mois. La Commission prend acte que cet allongement de la durée de traitement des demandes est rendu nécessaire par l'augmentation constante du nombre de demandes dont sont saisis les procureurs de la République et l'exigence d'un examen approfondi des dossiers. Elle souligne néanmoins que les mesures nécessaires doivent être prises pour que ce délai de deux mois soit respecté de manière effective, afin d'assurer le bon exercice des droits des personnes concernées.

Article 27 (Application aux PTOM)

L'article 27 du projet de loi a pour objet de modifier l'article 72 de la loi du 6 janvier 1978 afin de rendre applicables les dispositions de cette loi aux pays et territoires d'outre-mer (PTOM).

La Commission relève néanmoins que les dispositions du Règlement, qui sont directement applicables et auront vocation à se substituer aux dispositions de la loi du 6 janvier 1978, ne sont pas applicables aux PTOM, hors de son champ d'application. L'article 27 du projet n'a pas davantage pour effet de leur étendre le bénéfice de droits ou garanties en substance identiques à ceux du Règlement. L'ordonnance à venir devra, conformément à l'habilitation prévue à l'article 23, résorber ce décalage.

Article 28 (Entrée en vigueur)

La Commission n'émet pas d'observation sur cet article.

La Présidente

Isabelle FALQUE-PIERROTIN