N° 592

———

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 25 janvier 2018

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE, SUR LE PROJET DE LOI

relatif à la **protection** *des* **données personnelles** (n° 490),

PAR MME PAULA FORTEZA

Députée

———

Voir les numéros :

Assemblée nationale : **577** et **579**.

SOMMAIRE

___

Pages

MESDAMES, MESSIEURS,

La collecte, l'analyse et le traitement des données personnelles sont devenus la pierre angulaire de nombreux modèles d'affaires qui répondent à des pratiques très ancrées dans nos sociétés contemporaines et qui ne cesseront de se développer dans les années à venir. Les nouvelles technologies à disposition (« *cloud computing* », internet des objets, intelligence artificielle) redéfinissent en permanence les contours de cette « économie de la donnée » en plein essor. La problématique de la protection des données personnelles se trouve ainsi actuellement **à la croisée entre respect des droits des personnes et régulation économique**. Le cadre juridique sur lequel le législateur est amené à se prononcer cristallise cette interdépendance croissante qui doit être appréhendée sous l'angle de la construction d'une politique numérique ambitieuse pour la France et pour l'Europe.

La protection des données personnelles et le droit au respect de la vie privée :

Qu'il s'applique au monde « physique » ou à l'univers numérique, dont les frontières respectives tendent à s'estomper, le droit au respect de la vie privée consiste à « *assure*[r] *à l'individu un domaine dans lequel il peut poursuivre librement le développement et l'accomplissement de sa personnalité* », comme l'a souligné dès 1977 la Cour européenne des droits de l'homme [(1)].

Protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 et l'article 8 de la Convention européenne des droits de l'homme, ce droit implique la protection de chaque personne face aux activités, publiques comme privées, de traitement des données qui la concernent. Cet impératif a conduit l'Union européenne (UE) à faire de la protection des données à caractère personnel un droit fondamental dans son ordre juridique, distinct du droit au respect de la vie privée [(2)], et à renforcer sa législation en la matière [(3)].

La France, l'un des tous premiers pays à s'être doté, le 6 janvier 1978, d'une loi relative à « *l'informatique, aux fichiers et aux libertés* », est appelée à adapter cette loi fondatrice, déjà actualisée en 2004 pour tenir compte d'une directive

---

(1) CEDH, 12 juillet 1977, Bruggemann et Scheuten c. RFA*, n° 6959/75.*

(2) L'article 8 de la Charte européenne des droits fondamentaux de l'Union européenne du 7 décembre 2000, à laquelle le traité de Lisbonne du 13 décembre 2007 a conféré valeur juridique contraignante, prévoit, en son article 7, que les données à caractère personnel « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi *», que «* toute personne a le droit d'accéder aux données la concernant et d'en obtenir la rectification *», et que «* le respect de ces règles est soumis au contrôle d'une autorité indépendante *».*

(3) L'article 16 du traité sur le fonctionnement de l'Union européenne consacre aussi ce droit et prévoit l'adoption, selon la procédure législative ordinaire, des règles relatives à la protection des personnes à l'égard du traitement de leurs données personnelles et à la libre circulation de leurs données.

de 1995, au nouveau cadre juridique dont s'est dotée l'Union européenne le 27 avril 2016.

Ce nouveau cadre, dénommé **« paquet européen de protection des données »**, se compose de deux textes : le règlement (UE) 2016/679 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, directement applicable à compter du 25 mai 2018 ; la 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, qui doit être transposée au plus tard le 6 mai 2018.

Ces textes remplacent des instruments qui n'avaient permis, jusqu'à présent, qu'une harmonisation imparfaite et partielle des législations nationales applicables en la matière. Ils sont le fruit d'un long processus, initié en 2009 par une consultation publique lancée par la Commission européenne, prolongé en 2010 par la publication d'une communication fixant les objectifs d'une nouvelle législation globale et parachevé en janvier 2012 avec le dépôt de deux propositions qui ont été adoptées au terme de quatre années d'intenses négociations. Durant cette période, **la France s'est opposée à tout recul par rapport au niveau de protection des droits des personnes assuré par la directive de 1995**, notamment s'agissant de la création d'une catégorie distincte pour les « données pseudonymisées ». La France a également soutenu l'approche fondée sur l'analyse des risques et la responsabilisation des entreprises, le renforcement des sanctions et l'instauration d'un mécanisme de régulation compatible avec l'exigence de proximité des personnes concernées avec leur autorité de protection et leurs juridictions.

Le « paquet européen de protection des données » a pour ambition de **tirer les conséquences des nouvelles pratiques numériques** – progression des moyens de captation, de stockage, de reproduction et d'analyse des données, explosion du volume de données traitées (big data), essor de l'internet, des objets et de l'intelligence artificielle, valorisation intensive des données personnelles disponibles, multiplication des pratiques de partage d'informations, d'opinions ou de publications sur des plateformes ou réseaux – et des bouleversements qui sont intervenus dans la conception de la vie privée et de la valeur attachée à sa protection.

Dans ce contexte, toute personne doit pouvoir disposer « *du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant* », comme le prévoit, depuis la loi pour une République numérique du 7 octobre 2016, l'article 1er de la loi du 6 janvier 1978. Ce « **droit à l'autodétermination informationnelle** » (1), qui écarte toute logique patrimoniale dans la protection des données personnelles, se traduit, dans le « paquet européen », par une nouvelle philosophie de protection des personnes concernées. C'est plus globalement l'économie générale de la législation relative à la protection des données

(1) L'expression a été utilisée pour la première fois par la Cour constitutionnelle fédérale allemande dans un arrêt du 15 décembre 1983 relatif à une loi sur le recensement.

personnelles qui se trouve redéfinie, à travers une responsabilisation accrue des acteurs et une redéfinition du rôle de la régulation.

La protection des données personnelles et la régulation de l'écosystème du numérique :

Les **impacts économiques** du cadre juridique qui découle du « paquet européen de la protection des données » sont multiples. Ils concernent notamment la promotion de l'innovation et de l'entreprenariat, la remise à niveau du « terrain de jeu » pour les petites et moyennes entreprises, le développement d'une concurrence loyale pour les entreprises européennes, et l'émergence de nouvelles compétences.

Le changement de paradigme d'un régime d'autorisation préalable vers un régime de responsabilisation des acteurs, ainsi que l'appel à des outils de droit souple tels que les référentiels, les codes de bonne conduite et les packs de conformité, sont un **gage d'allègement des démarches administratives et de réduction des délais de mise en œuvre pour les entreprises**. Il s'agit, dans un contexte incertain et dans lequel les avancées techniques sont toujours plus rapides que la capacité du législateur à en évaluer les impacts, de construire les cadres régulateurs de façon plus flexible, itérative et collaborative pour qu'ils soient adaptés aux enjeux du numérique et qu'ils deviennent de véritables « aides à la mise en conformité ». L'**homogénéisation des normes au niveau européen** concourt aussi à clarifier le droit applicable tant pour les citoyens et les consommateurs que pour les entreprises.

Le cadre juridique proposé attribue aux autorités de contrôle un **nouveau rôle d'accompagnement des entreprises**, plus particulièrement des petites et moyennes entreprises. Les responsabilités des sous-traitants – pour la plupart des petites et moyennes entreprises qui assurent le traitement effectif des données – seront précisées de façon plus claire et détaillée. De nouveaux outils ont d'ailleurs commencé à être développés par différents acteurs pour accroître la **lisibilité des textes** qui rentreront en vigueur (https://donnees-personnelles.parlement-ouvert.fr/) ou faciliter la prise en main des nouvelles obligations (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil). L'enjeu est important : c'est la considération des difficultés particulières de ces acteurs à se mettre en conformité qui est la clé de voute pour transformer l'adaptation aux nouvelles dispositions en atout économique et en véritable valeur ajoutée aux yeux non seulement des citoyens mais aussi des consommateurs de biens et de services numériques.

L'innovation et l'entreprenariat sont favorisés par une simplification des démarches et par un accompagnement des entreprises, mais aussi par un renforcement de la **concurrence loyale**. Le droit à la **portabilité des données**, par exemple, permettra de contourner la « dépendance au sentier » qui prime dans l'industrie du numérique pour permettre à de nouvelles entreprises d'accéder à l'ensemble des données d'un consommateur et offrir des services alternatifs comparables. Par ailleurs, l'**extra-territorialité** des dispositions du « paquet européen » protègera les entreprises européennes face à la concurrence d'entreprises étrangères qui pouvaient auparavant proposer des services aux citoyens européens sans être tenues de respecter le droit

local en matière de protection des données personnelles. Cela permettra aussi, par ruissèlement, de rehausser les standards de protection en dehors de l'Union Européenne.

L'élargissement des missions des autorités de contrôle, la création des délégués à la protection des données personnelles (DPO) – figure dorénavant obligatoire tant dans les entreprises que dans les administrations et les collectivités territoriales – et l'émergence d'une activité de conseil spécialisée dans le secteur de la protection des données personnelles, contribue à consolider et à diffuser dans tous les secteurs un nouveau profil de compétences. La maîtrise cumulative du droit et de l'informatique devient un parcours professionnel valorisé, compétences qui sont, par ailleurs, essentielles à une industrie du numérique qui se veut protectrice et responsable.

Cette nouvelle attractivité économique et juridique est **une opportunité pour la France**, qui aura la possibilité de commencer à construire, dans le cadre européen, un modèle alternatif de croissance autour d'**une industrie numérique plus éthique, accessible et décentralisé** que le sont actuellement le modèle américain ou le modèle chinois.

Le débat de société sur la politique de la protection des données personnelle doit être élargi pour y inclure son interaction avec la politique numérique de la France au sens large ; ceci avait déjà été signalé par le Conseil d'État dans son avis [(1)]. Les échanges à venir autour du projet de Règlement ePrivacy, du marché unique numérique européen ou de la renégociation du « *Privacy Shield* » seront autant d'occasions pour **poursuivre cette réflexion collective**.

Le présent projet de loi a un objet plus circonscrit. D'une part, le règlement général sur la protection des données étant d'application immédiate, le texte vise seulement à éliminer de la loi de 1978 les dispositions qui lui sont contraires, à compléter celles qui doivent l'être afin de les rendre conformes aux exigences européennes et à transposer la directive sur les traitements de données personnelles en matière pénale. D'autre part, il intervient là où le règlement européen renvoie aux États membres le soin de préciser certaines dispositions ou leur laisse une marge d'appréciation.

Les implications importantes de ce texte ont conduit la commission des Affaires sociales à se saisir pour avis des dispositions intéressant les données de santé – en désignant, en qualité de rapporteure, Mme Albane Gaillot – et la commission des Affaires européennes à s'en saisir pour observations – en désignant Mme Christine Hennion.

Quelques semaines après le quarantième anniversaire de la loi « Informatique et libertés », publiée au *Journal officiel* le 6 janvier 1978, la commission des Lois est donc appelée à se prononcer sur un texte majeur qui va en redéfinir les équilibres et conduire, à terme, à sa réécriture d'ensemble.

---

(1) https://donnees-personnelles.parlement-ouvert.fr/avis-conseil-etat-393836

I. LE « PAQUET EUROPÉEN DE PROTECTION DES DONNÉES » : DEUX INSTRUMENTS POUR UN CADRE JURIDIQUE HARMONISÉ ET ADAPTÉ AUX NOUVELLES RÉALITÉS DU NUMÉRIQUE

A. UN RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES FONDÉ SUR UN CHANGEMENT DE PARADIGME

Le règlement 2016/679 est fondé sur un triple changement de la législation, en ce qui concerne les droits des personnes, la responsabilisation des acteurs et la crédibilité de la régulation.

1. Un renforcement des droits des personnes concernées

Les droits des personnes face aux traitements des données personnelles qui les concernent sont renforcés dans quatre directions.

a. Une évolution des données protégées

La liste des données sensibles, par principe interdites de traitement, est étendue aux **données biométriques et génétiques** ainsi qu'à celles relatives à l'**orientation sexuelle** des personnes (article 9).

Si les données des **personnes décédées** ne font pas l'objet d'une protection spécifique, les États peuvent prévoir des règles particulières, faculté qui a été utilisée de manière anticipée par la France avec l'introduction, par la loi pour une République numérique de 2016, d'un article 40-1 dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui définit le régime des droits et le devenir des données d'une personne après son décès [(1)].

b. Un consentement renforcé

Afin de lever l'ambiguïté née de l'exigence posée par la directive de 1995 d'un consentement donné « *indubitablement* » par la personne, est désormais posé le principe d'un consentement **explicite**, sous la forme d'une « *manifestation de volonté, libre, spécifique, éclairée et univoque (...) par une déclaration ou par un acte positif clair* », ce consentement devant pouvoir être **retiré à tout moment** (article 4).

Des **conditions spécifiques s'appliqueront au recueil du consentement des enfants**. Seuls les mineurs âgés de plus de **16 ans** pourront donner personnellement leur consentement au traitement de leurs données. Pour ceux âgés

(1) Cet article prévoit l'extinction des droits « Informatique et libertés » au moment du décès de la personne, la possibilité pour les héritiers de régler la succession du défunt en ayant accès, comme cela se passe dans le monde physique, aux comptes du défunt aux seules fins d'obtenir les informations nécessaires à la succession et la communication des « valeurs » numériques (biens numériques et souvenirs de famille, y compris les correspondances) ainsi que la faculté pour les héritiers d'obtenir la clôture des comptes utilisateurs, la mise à jour ou l'arrêt des traitements.

de moins de 16 ans, le traitement ne sera licite que si le consentement a été donné par le titulaire de l'autorité parentale. Le règlement laisse la possibilité aux États d'abaisser ce seuil jusqu'à 13 ans, mais le Gouvernement a fait le choix de ne pas utiliser, pour la France, cette marge d'appréciation (article 8).

c. Un approfondissement et une extension des droits

S'agissant des droits de la personne concernée par le traitement, le **champ des informations devant être fournies est élargi** (1) (articles 13 et 14). Ces informations devront être **transmises « *d'une façon concise, transparente, compréhensible et aisément accessible**, en des termes clairs et simples* »** (article 12).

De surcroît, de **nouveaux droits** sont reconnus à la personne concernée :

— un **droit à la portabilité des données** (article 20), qui permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers ;

— un **droit à l'effacement des données** (article 17) dont les motifs sont élargis par rapport au droit actuel (2) et qui oblige à prendre « *des mesures raisonnables (...) pour informer les responsables du traitement qui traitent ces données (...) que la personne concernée a demandé l'effacement (...) de tout lien vers ces données (...), ou de toute copie ou reproduction de celles-ci* » ; ce droit à l'effacement est complété par le **droit au déréférencement** consacré par la Cour de justice de l'Union européenne en mai 2014 (3), qui permet de demander à un moteur de recherche de supprimer certains résultats associés aux noms et prénoms d'une personne ;

— un **droit à réparation du dommage matériel ou moral subi** du fait d'une violation du règlement par le responsable du traitement ou le sous-traitant (article 82) ;

— les **actions collectives** (article 80) : les associations actives dans le domaine de la protection des données pourront être mandatées par toute personne concernée pour introduire une réclamation auprès d'une autorité de contrôle, exercer un recours juridictionnel contre une autorité de contrôle ou contre un responsable de traitement ou un sous-traitant. D'autres modalités de recours

---

(1) Intérêts légitimes fondant le traitement, intention du responsable de traitement d'effectuer un transfert vers un pays tiers, durée ou critères de conservation des données, droit de demander l'effacement des données ou une limitation du traitement, existence d'une prise de décision automatisée, intention du responsable de traitement d'effectuer un traitement ultérieur pour d'autres finalités.

(2) Lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, ont fait l'objet d'un traitement illicite, doivent être effacées pour respecter une obligation légale ou ont été collectées auprès d'enfants ou bien lorsque la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique à celui-ci, s'oppose au traitement et qu'il n'existe pas de motif légitime impérieux pour le traitement ou s'oppose au traitement à des fins de prospection.

(3) CJUE, 13 mai 2014, Google Spain c. AEPD*, n° C-131/12.*

relèvent des marges de manœuvre des États membres : possibilité d'étendre le mandat défini précédemment afin d'exercer une action en réparation dans le cadre d'une action de groupe (article 80.1), possibilité pour un organisme, une organisation ou une association, d'exercer les droits définis ci- dessus, indépendamment de tout mandat confié par une personne concernée (article 80.2).

d. Une plus grande protection face au profilage

Les décisions individuelles automatisées faisaient déjà l'objet d'un encadrement par la directive de 1995 et la loi de 1978. Le règlement maintient le droit pour toute personne « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ». Est cependant ajoutée l'**exigence d'un consentement explicite comme fondement du profilage** ainsi qu'une marge de manœuvre en droit national (point 2. b) qui permet d'autoriser la prise de **décision individuelle automatisée**, à condition de prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée (article 22).

La personne concernée par un profilage devra également faire l'objet d'une **information spécifique**, sous la forme d'« *informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement* » (article 14).

2. Une responsabilisation accrue des acteurs

Le renforcement des droits de la personne concernée s'accompagne d'un bouleversement des principes s'imposant aux acteurs traitant des données personnelles, au travers du **passage d'une logique de formalités préalables** (déclarations et autorisations) **à une logique de conformité et de responsabilité**.

Hors les cas dans lesquels le droit national peut maintenir des autorisations pour certaines catégories de données ou de traitements, sont **supprimées la plupart des obligations déclaratives et des autorisations préalables** exigées avant la mise en œuvre de traitements de données personnelles au profit de l'obligation de réaliser une analyse de l'impact des opérations sur la protection des donnés en cas de risque élevé pour les droits et libertés des personnes (article 35). De manière plus générale est instaurée une obligation de mettre en œuvre « *des **mesures techniques et organisationnelles appropriées** pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au (…) règlement* » (article 24).

Cet allègement des formalités a pour contrepartie l'établissement de **nouvelles obligations** pesant sur les responsables de traitements et sous-traitants, comme la mise en œuvre d'outils de protection des données personnelles dès la conception du traitement ou par défaut (article 25), la désignation d'un délégué à la protection des données (article 37), l'obligation de tenir une documentation, en

particulier au travers d'un registre des activités de traitement (article 30), la participation à des mécanismes de certification (articles 42 et 43), l'adhésion à des codes de bonne conduite (articles 40 et 41) ou encore la notification des violations de données personnelles à l'autorité de protection et, dans certains cas, à la personne concernée (articles 33 et 34).

3. Une plus grande crédibilité de la régulation

En dernier lieu, le règlement européen améliore de manière significative l'efficacité de la régulation des activités de traitement de données personnelles.

a. Un champ d'application élargi

Le périmètre d'application de la législation est géographiquement étendu aux entreprises qui ne sont pas établies sur le territoire de l'Union européenne (UE) mais qui traitent des données de personnes s'y trouvant, dès lors que ces activités de traitement sont liées à une offre à ces personnes de biens ou de services, qu'un paiement soit exigé ou non, ou dès lors que le traitement est lié au suivi de leur comportement (article 3).

Matériellement, la **responsabilité conjointe des responsables de traitements et des sous-traitants** pourra être engagée en cas de manquement, ces deux catégories d'acteurs étant désormais soumises, la plupart du temps, aux mêmes obligations.

b. Des sanctions administratives alourdies

Les mécanismes de sanction du non-respect des obligations sont considérablement renforcés, alors que le montant maximal des amendes susceptibles d'être prononcées en application du droit antérieur – 150 000 euros – était insuffisamment dissuasif, même si la loi pour une République numérique avait porté ce plafond à 3 millions d'euros.

Les autorités de contrôle pourront désormais prononcer, en complément ou à la place des mesures correctives (mises en demeure, limitation du traitement, suspension des flux de données…), des **amendes administratives pouvant atteindre**, selon la catégorie du manquement, **10 à 20 millions d'euros** ou, dans le cas d'une entreprise, **2 % à 4 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu (article 83).

c. La coopération des autorités de contrôle nationales

Enfin, le règlement instaure un mécanisme de décisions conjointes des autorités de contrôle nationales. Les responsables de traitements ne rendront compte qu'à une seule autorité de contrôle au sein de l'Union, celle du pays où ils disposent de leur établissement principal, appelée **autorité « chef de file »** (article 56).

En présence d'un traitement transnational concernant des personnes se trouvant dans plusieurs États membres, une **réponse unique, issue d'une coopération des autorités concernées,** sera apportée, mettant ainsi un terme aux pratiques de *forum shopping*, consistant dans la recherche des juridictions les plus favorables. En pratique, l'autorité « chef de file » proposera les mesures ou décisions de conformité ou de non-conformité d'un traitement. Puis les autres autorités européennes concernées disposeront d'un délai de quatre semaines pour approuver cette décision ou soulever une objection. Si l'objection n'est pas retenue par l'autorité « chef de file », la question devra être portée devant le Comité européen de protection des données, qui réunira, comme le fait aujourd'hui le « G29 », les autorités de protection nationales et dont l'avis s'imposera. Au final, une décision conjointe sera réputée prise, susceptible de recours devant le juge des décisions de l'autorité « chef de file » (article 60).

B. UNE DIRECTIVE RENFORÇANT L'ENCADREMENT DES FICHIERS DE LA SPHÈRE PÉNALE

1. Un instrument juridique permettant une harmonisation du niveau de protection au sein de l'Union européenne et une coopération plus efficace

Le droit actuel se caractérise par une importante hétérogénéité des législations applicables aux traitements de données personnelles dans le domaine pénal. Le seul instrument juridique européen adopté en la matière était une décision-cadre de 2008 [(1)], dont le champ était toutefois limité aux échanges entre États membres de l'Union européenne ou entre ces États et des États tiers, les traitements de fichiers nationaux demeurant soumis aux législations nationales.

L'adoption de la directive (UE) 2016/680 constitue un progrès notable dans l'harmonisation des règles applicables à cette catégorie de traitements, à défaut d'avoir un texte unique fusionnant les dispositions de la directive et du règlement. L'existence d'un texte distinct du règlement et qui, à la différence de celui-ci, n'est pas d'application directe, s'explique non seulement par les difficultés juridiques et politiques liées aux positions du Royaume-Uni, de l'Irlande et du Danemark sur ce sujet mais aussi à la spécificité des fichiers en cause au regard de leur finalité et de la nature publique du responsable du traitement des données.

En tout état de cause, cette directive permettra **de garantir un même niveau de protection pour les personnes dans l'ensemble de l'Union européenne et d'éviter que des divergences de réglementation n'entravent les échanges de données.** Seront concernés par ces nouvelles règles tous les fichiers de police et de justice utiles à la prévention, à la poursuite et à la répression des infractions pénales ainsi qu'à leur exécution, y compris la protection contre les

(1) Décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

menaces à la sécurité publique, mais pas les fichiers de renseignement qui ne relèvent pas du droit de l'Union.

2. Des règles en partie identiques à celles du règlement général sur la protection des données

Les principes directeurs du règlement général sur la protection des données irriguent le contenu de la directive, qui comporte en conséquence de nombreuses dispositions identiques ou similaires, à commencer par les **principes relatifs aux traitements** que sont la licéité et la loyauté, l'existence de finalités déterminées, explicites et légitimes, le traitement de manière adéquate, pertinente, non excessive des données et dans des conditions garantissant leur exactitude, leur sécurité et leur conservation pendant une durée raisonnable (article 4).

Les personnes investies de l'autorité publique ou les organismes à qui a été confié l'exercice de prérogatives de puissance publique ainsi que les responsables de traitement concernés se trouveront soumis à des **obligations comparables à celles qui s'appliquent aux entreprises** : exigence de protection des données dès la conception et par défaut (article 20) ; obligation de tenir un registre des activités de traitement (article 24), d'effectuer une analyse d'impact en cas de risque élevé pour les droits et libertés de la personne concernée (article 27), de notifier à l'autorité de contrôle ou de communiquer à la personne les violations de données personnelles qui la concernent (articles 30 et 31) ou de désigner un délégué à la protection des données (article 32).

La personne disposera également de **droits** à l'égard du traitement des données qui la concernent, comme le droit **à l'information** (article 13), le droit **d'accès** (article 14), les droits **de rectification ou d'effacement** des données et **de limitation** du traitement (article 16). L'exercice de ces droits se fera **de manière directe, gratuite et accessible** (article 12). La nature des traitements en cause justifie en revanche que le droit d'opposition ne figure pas dans cette liste.

3. Une prise en compte de la sensibilité particulière de la matière pénale et des besoins spécifiques des autorités répressives

La directive se distingue du règlement en raison de la nécessité de prendre en compte le caractère sensible des fichiers en cause et les exigences propres à la matière pénale.

C'est la raison pour laquelle l'article 29 de la directive dresse une **liste exigeante des mesures techniques et organisationnelles** que le responsable du traitement ou le sous-traitant devra mettre en œuvre **afin de garantir un niveau de sécurité adapté au risque**, en particulier contre toute introduction frauduleuse dans le système ou toute lecture, copie, modification ou suppression non autorisées de données.

Par ailleurs, les traitements pénaux devront, dans la mesure du possible et en vue de se conformer au **principe d'exactitude**, opérer des **distinctions claires**, notamment **entre les données de différentes catégories de personnes concernées** –mises en cause, coupables, victimes et tiers – (article 6) ainsi qu'**entre les données fondées sur des faits et celles fondées sur des appréciations personnelles** (article 7).

Enfin, les États conservent la **possibilité de retarder ou de limiter, en totalité ou en partie, les droits de la personne concernée** afin d'éviter que l'exercice de ceux-ci ne porte préjudice à l'efficacité de la prévention ou de la détection des infractions pénales ou ne nuise à la sécurité ainsi qu'aux droits et libertés d'autrui, à condition que cette limitation « *constitue une mesure nécessaire et proportionnée* » (articles 13, 15 et 16). La personne conservera néanmoins la possibilité d'exercer ses droits de manière indirecte et de former un recours juridictionnel (article 17).

C. DES ÉVOLUTIONS AUX INCIDENCES MAJEURES SUR LES ACTEURS

Ce nouveau cadre juridique est appelé à remplacer les dispositions en vigueur dans le courant du mois de mai 2018, le règlement devenant directement applicable le 25 mai et la directive devant être transposée au plus tard le 6 du même mois. Les acteurs concernés doivent donc se mettre en conformité avec ces nouvelles règles qui dessinent une conception spécifiquement européenne de la protection des données.

1. Le coût de la mise en conformité

Si certains acteurs ont d'ores et déjà anticipé ces évolutions, d'autres devront faire en sorte de respecter les nouvelles obligations posées, notamment, par le règlement. Cette mise en conformité aura un **coût économique pour les entreprises** et un **coût budgétaire pour l'État et les collectivités territoriales**.

La **situation des très petites entreprises (TPE) et des petites et moyennes entreprises (PME)** doit être prise en considération puisqu'elles ne bénéficient que d'une seule dérogation, celle applicable aux organisations comptant moins de 250 employés en ce qui concerne la tenue de registres (article 30). Le règlement encourage d'ailleurs à l'élaboration de codes de conduite et à la mise en place de mécanismes de certification en matière de protection des données en vue de contribuer à la bonne application de la législation par les micro, petites et moyennes entreprises, en tenant compte de leurs besoins spécifiques (articles 40 et 42).

Votre rapporteure ne peut que souscrire à cette démarche d'accompagnement. Elle se félicite que la CNIL ait annoncé, au cours de son audition, qu'elle tiendrait compte du nécessaire **délai d'apprentissage** et rendrait public un **« pack PME-TPE » sur la mise en conformité au règlement**, également utile pour le secteur associatif. Ces initiatives s'inscrivent en

complément de celles déjà prises, comme l'ouverture sur le site de la CNIL d'une page dédiée à la préparation au règlement européen, la publication de méthodes, l'envoi de courriers de sensibilisation aux organisations professionnelles représentant les secteurs d'activités concernés, la mise en ligne d'un logiciel *open source* PIA pour faciliter la conduite et la formalisation d'analyses d'impact. Elles sont complétées par la diffusion des **lignes directrices du G29** clarifiant et illustrant le nouveau cadre juridique en matière d'autorité « chef de file », de délégué à la protection des données, de portabilité ou d'analyse d'impact.

2. La protection des données personnelles, une source d'attractivité et un avantage concurrentiel

Les nouvelles règles sont aussi **sources de réduction des charges administratives**, comme la suppression des notifications préalables, formalité qui représente, selon la Commission européenne, un coût de 130 millions d'euros par an pour les entreprises, ou la possibilité d'exiger le paiement d'une somme pour répondre aux demandes d'accès à des données manifestement infondées ou excessives. Les PME et TPE pourront également être exemptées de l'obligation de désigner un délégué à la protection des données dès lors que le traitement des données constitue pour elles une activité auxiliaire et n'est pas leur cœur de métier. Elles ne seront pas obligées de procéder à une analyse d'impact, à moins qu'il existe un risque élevé pour les droits et libertés des personnes.

Loin d'être une entrave à l'activité économique, le règlement et la directive, en portant une conception spécifiquement européenne de la protection des données personnelles, différente de celle promue par les États-Unis dont sont issus nombre des entreprises concernées, représente un **avantage concurrentiel dans la compétition économique**. L'Union européenne, important marché de consommateurs dans le domaine du numérique, devient un espace homogène en matière de protection des données personnelles, permettant aux acteurs économiques d'aller au-delà d'une simple logique de mise en conformité et de se démarquer de la concurrence : la **protection de la confidentialité et de la sécurité des données est appelée à être un moyen de différenciation vis-à-vis du consommateur**. De ce point de vue, votre rapporteure observe que la France a, au travers de sa culture de protection des données et de son expertise juridique ancienne dans ce domaine, des atouts à faire valoir dans l'application des nouvelles règles. Plusieurs pays, comme l'Inde, la Tunisie, l'Argentine, le Chili ou la Jamaïque s'inspirent d'ailleurs de la législation européenne en matière de protection des données personnelles.

Cela étant, l'entrée en vigueur prochaine de ce « paquet européen » et l'examen du présent projet de loi n'épuisent pas les discussions sur la société numérique :

— la question du transfert des données des usagers européens vers les entreprises américaines, qui a fait l'objet du nouvel accord avec les États-Unis dénommé **« Bouclier vie privée Union européenne – États-Unis »** (*EU-US*

Privacy Shield), après l'invalidation du précédent accord « Sphère de sécurité » (*Safe Harbor*) par la Cour de justice de l'Union européenne [(1)], sera prochainement tranché par cette dernière après le recours déposé par plusieurs associations contre cet accord ;

— au-delà, l'approfondissement de l'espace européen commun des données se poursuivra par l'adoption, dans les années à venir, d'un **règlement relatif à la libre circulation des données à caractère personnel et d'un règlement « vie privée et communications électroniques** (« *e-privacy* »).

II. LA NÉCESSAIRE ADAPTATION DE NOTRE DROIT À CES ÉVOLUTIONS, SOUS RÉSERVE DES MARGES D'APPRÉCIATION LAISSÉES AUX ÉTATS

La portée du présent projet de loi est circonscrite par la nature juridique du règlement général sur la protection des données : il vise à rendre conformes au règlement et à la directive celles des dispositions de notre droit qui leur sont contraires et à en préciser les modalités d'application lorsque l'un de ces textes renvoie au droit des États ou leur permet de prévoir des règles différentes.

L'ampleur des corrections techniques à opérer dans la loi de 1978 et dans d'autres textes législatifs a cependant conduit le Gouvernement à prévoir une habilitation à légiférer par ordonnance.

A. UNE MISE EN CONFORMITÉ DES DISPOSITIONS NATIONALES

1. L'adaptation du rôle de la CNIL

Les **articles 1er à 6** modifient la composition, les missions et les prérogatives de la CNIL, notamment pour les adapter aux nouvelles exigences européennes.

Il est ainsi prévu d'**enrichir ses missions afin de les inscrire encore davantage dans la nouvelle logique d'accompagnement des acteurs**, par l'établissement d'outils de droit souple destinés à faciliter la mise en conformité (lignes directrices, recommandations, référentiels), l'encouragement de la production de codes de conduite, l'élargissement du champ des mécanismes de certification et la production de règlements types en vue d'assurer la sécurité des systèmes de traitement. La CNIL pourra également être **consultée par le président de l'Assemblée nationale et du Sénat sur toute proposition de loi relative à la protection des données personnelles** (article 1er).

Outre l'inscription dans la loi de garanties d'impartialité dans la mise en œuvre de ses pouvoirs de sanction, la CNIL voit ses **prérogatives de contrôle étendues et précisées** (articles 3 et 4) : nature des locaux contrôlés, pouvoir de

(1) CJUE, 6 octobre 2015, Schrems*, n° C-362/14, voir le commentaire de l'article 17 dans le présent rapport.*

communication, opposition du secret professionnel, utilisation d'une identité d'emprunt. Sont également précisées les **modalités de la procédure de coopération entre la CNIL et les autres autorités de contrôle européennes**, en particulier s'agissant des pouvoirs de vérification et d'enquête reconnus aux membres et agents de ces autorités sur le territoire national (article 5).

Enfin, sont adaptées la possibilité actuellement reconnue à la CNIL de prononcer des **mesures correctrices** à l'encontre de responsables de traitement ne respectant pas leurs obligations, la répartition des pouvoirs entre le président et la formation restreinte, la nature des sanctions complémentaires, les mesures pouvant être prises par la formation restreinte en cas d'urgence ou l'augmentation du montant des sanctions pécuniaires (article 6).

2. L'élargissement du champ des données dites « sensibles »

Conformément aux dispositions du « paquet européen », l'**article 7** maintient le principe d'**interdiction des traitements de données sensibles**, applicable à tous les traitements portant sur ces données, qu'ils relèvent du droit de l'Union européenne ou du droit national, mais **étend le champ de cette interdiction aux données génétiques et biométriques ainsi qu'aux données concernant l'orientation sexuelle** d'une personne.

Des **dérogations** sont prévues par l'article 9 du règlement européen, auxquelles le projet de loi ajoute une dérogation pour les traitements mis en œuvre par les employeurs ou administrations aux fins, notamment, de contrôler l'accès aux lieux de travail, et celle actuellement prévue pour les traitements mis en œuvre par l'État, notamment en matière de données génétiques et biométriques, justifiés par l'intérêt public.

3. La transposition de la directive sur les traitements en matière pénale

Les **articles 18** et **19** transposent les dispositions de la directive sur les traitements de données personnelles en matière pénale.

Par souci de lisibilité, un nouveau chapitre dédié à ces traitements est inséré dans la loi de 1978, qui recense les principes généraux applicables à ces traitements, les obligations incombant aux autorités et responsables de ces traitements, les droits reconnus aux personnes concernées, assortis des restrictions susceptibles d'affecter leur portée ou leur exercice, ainsi que les conditions de transferts des données vers des États n'appartenant pas à l'Union européenne.

Les principales innovations induites par cette transposition consistent dans la **création d'un droit à l'information** de la personne dont les données sont traitées, l'**exercice en principe direct des droits reconnus à la personne concernée** (droit à l'information, droits d'accès, de rectification et d'effacement), la définition des motifs pouvant justifier que des **restrictions** soient apportées à

ces droits ainsi que l'encadrement des transferts de données vers des pays n'appartenant pas à l'Union européenne.

B. L'UTILISATION DES MARGES DE MANŒUVRE PERMISES PAR LE RÈGLEMENT

Dix articles du projet de loi exploitent les marges de manœuvre permises par le règlement général sur la protection des données, règlement *sui generis* qui, bien que d'application directe, compte plus de cinquante dispositions renvoyant au droit des États. Lors de son audition par votre rapporteure, la CNIL a souligné la nécessité de n'utiliser ces marges de manœuvre que lorsqu'un motif dirimant le justifiait.

1. Le maintien de formalités préalables pour certains traitements

Conformément au règlement européen, le projet de loi **simplifie, en les supprimant la plupart du temps, les formalités préalables imposées par la loi de 1978**, qu'il s'agisse des obligations de déclaration ou d'autorisation. Ces formalités seront remplacées par l'obligation, pour le responsable du traitement, d'effectuer préalablement une analyse d'impact en cas de risque élevé pour les droits et libertés de la personne concernée et, le cas échéant, de consulter la CNIL.

Toutefois, comme l'autorise le règlement, **le projet de loi maintient des formalités préalables pour certains traitements** :

— les **traitements mis en œuvre pour le compte de l'État qui intéressent la sûreté de celui-ci, la défense, la sécurité publique ou qui ont pour objet la prévention et la répression des infractions pénales**, qui resteront soumis au régime d'autorisation de l'article 26 de la loi de 1978 (**articles 9 et 19**) ;

— les **traitements de données biométriques – auxquelles sont ajoutées les données génétiques – pour le compte de l'État**, qui continueront d'être **autorisés par décret en Conseil d'État** après avis de la CNIL (**article 9**) ;

— les **traitements de données de santé**, qui feront l'objet d'un **régime *ad hoc***, soumettant leur mise en œuvre à une déclaration à la CNIL de conformité à des référentiels et règlements types ou, à défaut, à l'autorisation préalable de celle-ci, sauf en matière de recherche, d'étude ou d'évaluation dans le domaine de la santé (**article 13**) ;

— les **traitements, pour le compte de personnes publiques ou privées, de données comportant le numéro d'inscription des personnes (NIR)** au répertoire national d'identification des personnes physiques (RNIPP), qui devront être autorisés par un **« décret-cadre » en Conseil d'État**, sauf pour ceux ayant pour seules finalités la statistique publique, la recherche scientifique ou historique ou la mise à disposition de téléservices de l'administration (**article 9**).

2. Des dérogations aux droits des personnes concernées

Une autre marge de manœuvre donnée par le règlement européen conduit le Gouvernement à proposer d'**ouvrir plus largement le recours, en principe proscrit, de l'administration à des décisions individuelles automatisées**, c'est-à-dire prises à l'aide d'algorithmes, sous réserve de respecter certaines garanties (**article 14**). La loi pour une République numérique de 2016 avait reconnu, dans ce domaine, un droit d'accès des personnes aux règles définissant le traitement algorithmique ainsi qu'aux principales caractéristiques de sa mise en œuvre au bénéfice de l'usager.

Une autre disposition exploite la possibilité laissée aux États de limiter les droits de la personne concernée en vue de garantir certains objectifs d'intérêt public. L'**article 15** confie ainsi à un décret en Conseil d'État le soin de déterminer la liste des traitements autorisés à **déroger au droit à la communication d'une violation des données personnelles** lorsque cette communication « *est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique* ».

3. Les actions de groupe

Enfin, l'**article 16** précise les modalités du droit reconnu à toute personne par le règlement européen de mandater une association active en matière de protection de la vie privée, une association de défense des consommateurs ou une organisation syndicale pour qu'elle exerce en son nom certains droits, à l'exclusion de celui d'obtenir réparation du préjudice subi. Sont concernés le droit d'**introduire une réclamation auprès de la CNIL** et celui **de former un recours juridictionnel contre cette dernière ou contre un responsable de traitement ou un sous-traitant**. Cette disposition sera également applicable aux actions devant la CNIL, contre celle-ci devant un juge ou contre un responsable de traitement ou un sous-traitant pour les traitements de données en matière pénale.

Néanmoins, il n'est pas proposé d'utiliser la marge de manœuvre offerte par l'article 80.1 permettant une action de groupe pour obtenir réparation en cas de dommages causés par un responsable de traitement ni celle offerte par l'article 80.2 permettant une action de groupe en dehors de tout mandat en cas de violation des articles 77 et 78 du règlement.

C. LA MISE EN COHÉRENCE, PAR ORDONNANCE, DE LA LÉGISLATION RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES

Le Gouvernement a choisi de n'opérer, dans ce projet de loi, que les modifications de fond rendues indispensables par l'entrée en vigueur prochaine du règlement général sur la protection des données et la nécessité de transposer la directive sur les traitements de données en matière pénale d'ici le mois de mai 2018.

C'est la raison pour laquelle l'**article 20** habilite le Gouvernement à **procéder, par voie d'ordonnance prise après avis de la CNIL dans un délai de six mois, à la réécriture d'ensemble de la loi de 1978** et, le cas échéant, des textes connexes. L'objectif de cette ordonnance est « *d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées des dispositions qui mettent le droit national en conformité* » avec le « paquet européen » et d'« *assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions (…) et abroger les dispositions devenues sans objet* ».

Votre rapporteure rejoint le souhait formulé par nombre des personnes qu'elle a auditionnées et celui exprimé par la CNIL dans son avis sur le présent projet de loi d'une « *adoption des plus rapprochées de l'ordonnance annoncée, ainsi qu'une réécriture du droit français (…) de manière à ce que la loi du 6 janvier 1978 puisse donner un mode d'emploi clair* » (1) de la portée des droits et obligations nouvellement institués.

III. LES PRINCIPAUX APPORTS DE LA COMMISSION DES LOIS

A. LA MODIFICATION DE L'ÂGE DU CONSENTEMENT DES MINEURS

Sur proposition de votre rapporteure, la Commission a fait le choix d'utiliser la marge de manœuvre laissée par le règlement général sur la protection des données pour fixer l'âge à partir duquel un mineur peut consentir seul au traitement des données qui le concernent dans le cadre des services de la société de l'information, principalement les réseaux sociaux.

Le règlement a fixé par défaut cet âge à 16 ans tout en laissant aux États la possibilité d'y déroger pour l'abaisser jusqu'à 13 ans. Conformément à la position défendue par la France lors des négociations européennes, le Gouvernement avait fait le choix, dans le texte qu'il a présenté à l'Assemblée nationale, de ne pas utiliser cette marge de manœuvre.

Suivant l'avis de votre rapporteure qui a consulté de nombreux acteurs sur cette question (entreprises du numérique, associations protectrices de l'enfance…), **la Commission a décidé d'abaisser ce seuil à 15 ans** tout en posant l'exigence d'un double consentement des parents et du mineur en-dessous de cet âge et l'obligation pour les responsables de traitements de communiquer selon des modalités adaptées à l'âge du mineur (**article 14 A**).

---

(1) Délibération n° 2017-299 du 30 novembre 2017 de la CNIL portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978, p. 5.

Ces règles paraissent à votre rapporteure mieux **concilier l'exigence de protection des mineurs sur internet, la réalité des pratiques numériques actuelles et la nécessité de mieux accompagner les mineurs dans la découverte des réseaux sociaux**.

B. LA CLARIFICATION DES CONDITIONS ET DES GARANTIES MINIMALES APPLICABLES EN CAS DE MISE EN ŒUVRE D'UN TRAITEMENT ALGORITHMIQUE

Sur proposition de votre rapporteure, la **Commission a clarifié, à l'article 14, le principe selon lequel aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données sauf exceptions.**

Ces **exceptions** sont les suivantes :

1° **Les décisions résultant de la conclusion ou de l'exécution d'un contrat** entre la personne concernée et un responsable du traitement et **les décisions fondées sur le consentement explicite de la personne concernée** (exceptions mentionnés aux *a* et *c* du *2* de l'article 22 du règlement) dès lors que les **garanties minimales suivantes**, posées par le *3* du même article, sont assurées :

— droit de la personne concernée d'obtenir une **intervention humaine** de la part du responsable du traitement ;

— droit d'**exprimer son point de vue** ;

— droit de **contester la décision**.

2° **Les décisions administratives individuelles dès lors que les garanties minimales suivantes sont assurées :**

— le respect des obligations prévues par l'article L. 311-3-1 et par le chapitre 1er du titre Ier du livre IV du code des relations entre le public et l'administration (droit d'accès au code source, obligation générale d'information du public par l'administration des règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles, obligation d'information à l'égard de la personne concernée qu'elle fait l'objet d'une décision individuelle fondée sur un seul traitement algorithmique et qu'elle peut demander les principales caractéristiques de sa mise en œuvre par l'administration selon les modalités fixées par l'article R. 311-3-1-1) ;

— l'interdiction que le traitement porte sur des données sensibles au sens du I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 ;

— le **droit d'exercer un recours** comme pour toute décision administrative individuelle ;

— la **maîtrise du traitement algorithmique et de ses évolutions** par le responsable de traitement, **afin de pouvoir expliquer, en détails et sous une forme intelligible, à la personne concernée, la manière dont le traitement a été mis en œuvre à son égard**. Sont donc interdites les décisions administratives individuelles à partir d'un traitement fondé sur un algorithme auto-apprenant (algorithme « boite noire »).

C. L'ÉLARGISSEMENT DE L'ACTION DE GROUPE EN MATIÈRE DE DONNÉES PERSONNELLES À LA RÉPARATION DES PRÉJUDICES MATÉRIELS ET MORAUX

Sur proposition de votre rapporteure, la Commission a fait le choix d'utiliser la marge de manœuvre laissée par l'article 80, § 1, du règlement général sur la protection des données pour **étendre l'action de groupe** en constatation d'un manquement du responsable de traitement ou de son sous-traitant, introduite par la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle, **à l'action en réparation des préjudices matériels et moraux subis par la personne concernée** (**article 16 A**).

Ce choix est justifié pour au moins **deux raisons**. D'une part, l'action de groupe en matière de données personnelles était la **seule action de groupe prévue en droit français pour laquelle l'action en réparation n'était pas ouverte** ; d'autre part, l'action en réparation des dommages matériels et moraux permettra de **rendre l'action de groupe beaucoup plus effective en France**, même si d'autres mesures en complément pourraient être envisagées : les associations auditionnées ont en effet indiqué qu'elles n'étaient pas sollicitées par les personnes concernées dès lors que ces dernières ne pouvaient obtenir, par cette voie de recours, réparation des dommages causés par la violation de leurs données personnelles.

D. UNE MEILLEURE PRISE EN COMPTE DES SPÉCIFICITÉS DES PETITES ET MOYENNES ENTREPRISES

Conformément aux dispositions prévues par le règlement européen, la Commission a souhaité préciser que la CNIL doit, dans l'exercice de ses missions, et plus particulièrement dans le cadre de l'élaboration des codes de conduite et des procédures de certification, prendre en compte les besoins spécifiques des micro, petites et moyennes entreprises.

Si elle confirme en cela une pratique déjà à l'œuvre au sein de cette autorité, qui prête une attention particulière à l'adaptation des obligations faites aux responsables de traitement en fonction de leur taille et de leurs moyens, la responsabilisation des acteurs économiques et les conséquences des manquements qui pourraient être constatés justifient encore davantage une telle approche.

E. UNE PROTECTION RENFORCÉE DE CERTAINES DONNÉES SENSIBLES

Faisant usage de la marge de manœuvre prévue au 4 de l'article 9 du règlement européen selon lequel « *les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé* », la Commission a souhaité assurer un même niveau de protection pour ces données qui présentent, en effet, une sensibilité particulière.

Elle a ainsi étendu le champ des règlements types pouvant être pris par la CNIL pour régir les données de santé aux données biométriques et génétiques. Ces règlements pourront également porter sur des mesures plus larges que celles prévues par le projet de loi initial qui étaient restreintes à l'organisation ou aux techniques utilisées par les responsables de traitements.

F. LA SAISINE DE LA CNIL PAR LES COMMISSIONS PERMANENTES DES ASSEMBLEES PARLEMENTAIRES

De manière à renforcer l'expertise du Parlement, la Commission a souhaité élargir aux commissions permanentes des assemblées parlementaires la possibilité de saisir la CNIL sur toute proposition de loi portant sur la protection des données personnelles. Cette saisine était, en effet, réservée, dans le projet de loi initial, aux présidents de l'Assemblée nationale et du Sénat.

Les parlementaires seront ainsi en capacité de mieux appréhender les enjeux liés au numérique et à la protection des libertés individuelles, en amont de la modification des règles en vigueur.

DISCUSSION GÉNÉRALE

Lors de sa réunion du mardi 23 janvier 2018, la commission des Lois procède à l'audition de Mme Nicole Belloubet, garde des Sceaux, ministre de la Justice, et à la discussion générale sur le projet de loi (n° 490) relatif à la protection des données personnelles (Mme Paula Forteza, rapporteure).

Mme la présidente Yaël Braun-Pivet. Nous entamons ce soir l'examen du projet de loi relatif à la protection des données personnelles, déposé sur le bureau de l'Assemblée nationale le 13 décembre 2017.

Plusieurs rapporteurs ont travaillé sur ce texte : Mme Paula Forteza, rapporteure de la commission des Lois ; M. Philippe Gosselin, co-rapporteur d'application ; Mme Albane Gaillot, rapporteure pour avis de la commission des Affaires sociales ; Mme Christine Hennion, rapporteure de la commission des Affaires européennes, qui s'est saisie pour observations.

Nous avons le plaisir d'accueillir Mme Nicole Belloubet, garde des Sceaux, ministre de la Justice, à qui je donne la parole.

Mme Nicole Belloubet, garde des Sceaux, ministre de la Justice. Je suis très heureuse de retrouver la commission des Lois pour présenter ce projet de loi relatif à la protection des données personnelles, dont l'objet est d'adapter au droit de l'Union européenne (UE) la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Il est nécessaire, en effet, de transposer le nouveau cadre juridique européen, composé de deux textes : d'une part, le règlement 2016/679 et, d'autre part, la directive 2016/680. Ce cadre juridique entrera en vigueur en mai 2018.

Ces textes européens sont l'aboutissement d'une longue phase de réflexion et de négociations, et ils traduisent l'ambition très forte de notre continent dans le domaine de la protection des données à caractère personnel.

Cette protection constitue en effet l'une des dimensions nouvelles, de plus en plus importante au quotidien, du droit au respect de la vie privée. Elle est consacrée par la Charte des droits fondamentaux de l'Union européenne, en son article 8.

La France a toujours été très attentive et le plus souvent pionnière sur ces questions. Notre pays a ainsi été l'un des premiers en Europe à se doter non seulement d'une législation globale de protection des données à caractère personnel, avec la loi du 6 janvier 1978 dont nous venons de fêter les quarante ans, mais également d'une autorité de contrôle : la Commission nationale de l'informatique et des libertés (CNIL).

Le développement de l'ère numérique oblige cependant à repenser le cadre applicable aux données personnelles. Je n'ai pas besoin de souligner à quel point

le partage et la collecte de telles données connaissent un développement spectaculaire. C'est par ce biais que les nouvelles technologies transforment aujourd'hui profondément notre économie mais également les rapports sociaux qui nous lient.

Dans le même temps et très légitimement, la protection de leurs données constitue un motif de préoccupation croissante chez nos concitoyens. Selon une récente étude de l'institut CSA, 85 % des Français se disent préoccupés par la protection de leurs données personnelles en général, soit une augmentation de 4 points par rapport à 2014. Cette question suscite encore plus d'inquiétude dès lors qu'il s'agit de la protection des données sur internet : le pourcentage atteint alors 90 % des personnes interrogées, ce qui représente 5 points de progression par rapport à 2014. C'est une préoccupation largement partagée en Europe, car il s'agit là d'un phénomène qui ne connaît pas les frontières.

Devant de telles transformations, il était donc nécessaire que l'Union européenne envisage une évolution de la réglementation en la matière. C'est dans ce contexte que la Commission européenne a présenté, en janvier 2012, deux projets distincts définissant un nouveau cadre juridique applicable à la protection des données à caractère personnel.

La France a pris une part très active dans les négociations afin de maintenir et de promouvoir son modèle de protection, qui constitue encore aujourd'hui une référence en Europe et dans le monde. Dans le même temps, elle s'est préoccupée des conditions dans lesquelles les entreprises européennes, et plus particulièrement les petites et moyennes entreprises (PME), pourraient exercer leurs activités sans subir d'entraves excessives, notamment en matière de concurrence – je sais que c'est d'ailleurs l'une de vos préoccupations.

Fruit d'un compromis, le « paquet européen de protection des données » a été adopté par le Parlement européen et le Conseil le 27 avril 2016. Ce paquet se compose, d'une part, d'un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Applicable notamment à la matière civile et commerciale, il constitue le cadre général de la protection des données. Les obligations qu'il définit seront également applicables aux opérateurs installés hors de l'Union et offrant des biens et services aux Européens.

À ce règlement s'ajoute une directive, qui vise les traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Avant d'aborder la méthode retenue pour faire évoluer notre cadre juridique, permettez-moi de vous en dire un peu plus sur ces deux textes.

Le nouveau règlement crée un cadre unifié et protecteur pour les données personnelles des Européens, applicable à l'ensemble des entreprises et de leurs sous-traitants quelle que soit leur implantation, dès lors que ceux-ci offrent des

biens et services à des personnes résidant sur le territoire de l'Union européenne. C'est un point très important : le droit européen s'appliquera donc chaque fois qu'un résident européen, quelle que soit sa nationalité, sera directement visé par un traitement des données, y compris par internet ou par le biais d'objets connectés – par exemple, les montres connectées, les objets mesurant l'activité physique, les appareils domotiques, les consoles de jeux connectées – et ce, quelles que soient la nature et la localisation du support de stockage et de traitement.

Le règlement crée une procédure de coopération intégrée entre les autorités de protection des données des États membres – en France, la CNIL. Cela constitue un progrès majeur dans l'organisation de notre continent face à ces enjeux. Cette coopération intégrée permettra d'assurer une application uniforme des nouvelles obligations s'imposant aux opérateurs, notamment lorsqu'un traitement est transnational, sous l'égide du Comité européen de la protection des données.

Cette innovation permet à la France et à l'Union européenne de promouvoir l'affirmation d'une conception spécifique de la protection des données personnelles, conception qui diffère de celle promue notamment par les États-Unis. Cette conception européenne repose sur deux piliers : le renforcement de la confiance des citoyens dans l'utilisation qui est faite de leurs données personnelles d'abord, l'organisation, pour les opérateurs économiques, d'un environnement attractif, afin que l'Europe continue à donner l'exemple d'un continent qui sait concilier les valeurs de progrès et la protection des droits et libertés fondamentales.

Je reviens quelques instants sur ces deux points, et tout d'abord sur la mise en œuvre de nouveaux droits pour les citoyens. Le règlement conforte les droits des personnes physiques en matière de données les concernant déjà garantis dans la loi de 1978 – notamment le droit d'information – tout en instaurant de nouveaux droits pour les citoyens, en particulier un droit à la portabilité des données personnelles. Ce droit à la portabilité permet ainsi la récupération par les personnes concernées des données personnelles qu'elles ont fournies, dans un format réutilisable, ainsi que leur transmission à un autre responsable de traitement. Ce cadre juridique sécurisé permettra en conséquence de renforcer la confiance des citoyens dans l'utilisation qui est faite de leurs données personnelles.

Les incidences de ces nouvelles normes européennes en matière de protection des données personnelles sur la législation française ont d'ailleurs été très bien analysées dans le rapport de la mission d'information conduite par deux membres de la commission des Lois, Mme Anne-Yvonne Le Dain et M. Philippe Gosselin, présenté le 22 février 2017, sous la précédente législature. Ce rapport, comme d'autres contributions, a permis de nourrir les travaux conduits par la chancellerie pour rédiger le projet de loi qui vous est aujourd'hui soumis.

En second lieu, le règlement crée un environnement plus attractif pour des opérateurs économiques plus responsables. Ainsi que Mme Isabelle Falque-Pierrotin, présidente de la CNIL, a déjà eu l'occasion de le rappeler, le règlement européen inaugure une nouvelle ère dans la régulation, puisqu'il consacre un changement de paradigme : il s'agit d'alléger considérablement les formalités préalables au profit d'une démarche de responsabilisation des acteurs et d'un renforcement des droits des individus.

Ainsi, le nouveau règlement remplace le système de contrôle *a priori*, basé sur les régimes de déclaration et d'autorisation préalables, par un système de contrôle *a posteriori* plus adapté aux évolutions technologiques, fondé sur l'appréciation par le responsable du traitement des risques que présente ce dernier.

Cette responsabilisation des opérateurs, que ce soit le responsable du traitement lui-même ou son éventuel sous-traitant, selon un régime de responsabilité conjointe, s'incarne par de nouveaux principes : la « protection des données dès la conception » (*privacy by design*) et la « protection des données par défaut » (*privacy by default*). Ces principes imposent aux responsables de traitement d'intégrer les exigences de la protection des données personnelles très en amont de la conception de leur produit ou de leur service, et d'offrir au consommateur, par défaut, le niveau de protection le plus élevé.

Des analyses concernant l'impact des traitements sur la protection des données devront être conduites par les responsables de traitement lorsque celui-ci est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

La désignation d'un délégué à la protection des données sera obligatoire dans le secteur public. Elle le sera aussi lorsque l'activité principale d'une entreprise concerne le suivi, à grande échelle, régulier et systématique, des personnes, ou le traitement à grande échelle de données sensibles ou relatives à des condamnations.

Les responsables de traitement devront notifier les violations de données personnelles à l'autorité de contrôle ainsi qu'aux personnes concernées en cas de risque élevé pour leurs droits et libertés.

En responsabilisant les acteurs, le projet de loi consacre également de nouvelles modalités de régulation, à travers des outils de droit souple. Dans ce nouvel environnement juridique, la CNIL devra accompagner plus encore les acteurs, notamment les PME, qui doivent s'adapter aux nouvelles obligations en matière de protection des données.

En contrepartie, les pouvoirs de la CNIL sont renforcés et les sanctions encourues considérablement augmentées, puisqu'elles pourront être portées jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial consolidé d'une entreprise.

Le règlement général sur la protection des données (RGPD) met donc fin à la fragmentation des régimes juridiques au sein de l'UE, laquelle induisait un coût évalué par l'Union à 2,9 milliards d'euros par an pour les entreprises. Il entend instaurer un climat de confiance dans l'environnement en ligne, confiance essentielle au développement économique. Elle sera fondée sur un cadre juridique sécurisé pour les opérateurs, compatible avec le souci de soutenir l'attractivité de notre territoire, laquelle sera renforcée par un droit souple mais précis.

L'Union européenne représente aussi un marché de consommateurs important dans le domaine du numérique : il y a là un enjeu économique et technologique. Dans ce domaine, la France semble particulièrement bien armée, car elle peut faire valoir une culture de la protection des données et une véritable expertise juridique dans ce domaine, comme en témoigne son rôle important lors des négociations sur le règlement.

À côté du règlement, la directive fixe les règles applicables en matière pénale à la protection des personnes physiques, s'agissant du traitement des données à caractère personnel. C'est la première fois que l'Union se dote d'un cadre normatif pour réglementer le traitement de ces données au niveau national : auparavant, seuls les transferts de données d'un État membre à un autre étaient soumis à des règles européennes, formalisées dans la décision-cadre du 27 novembre 2008.

La directive s'applique aux traitements mis en œuvre par une autorité compétente à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Sont ainsi concernés, en France, les fichiers tels que le fichier national des empreintes génétiques, le fichier national des interdits de stade, ou encore le fameux TAJ – traitement des antécédents judiciaires.

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

Les principales innovations de la directive consistent en la création en matière pénale d'un droit à l'information de la personne concernée par les données personnelles traitées et en la consécration d'un droit d'accès, de rectification et d'effacement. Ces droits s'exercent, par principe, de manière directe par la personne concernée auprès du responsable de traitement, alors que la loi actuelle prévoit un exercice indirect de ces droits pour les traitements intéressant la sécurité publique et la police judiciaire.

Avec ce règlement et cette directive, le paquet européen se traduit donc par une modification profonde de notre mécanisme de protection des données personnelles. La France y a fortement contribué, avec pour objectif tout à la fois

de permettre à notre continent de répondre à ces nouveaux enjeux face aux autres acteurs mondiaux, étatiques ou non, et de promouvoir un modèle solide et opérationnel de protection des droits fondamentaux.

Néanmoins, le croisement de ces deux textes dans un domaine juridique complexe nous a contraints à faire des choix de méthode pour traduire le droit européen en droit français. Je voudrais m'y arrêter un instant car je sais que c'est une de vos préoccupations comme celle des acteurs concernés – et je peux vous assurer que c'est également la nôtre.

Rappelons que si la directive doit faire l'objet d'une transposition en droit interne, le règlement est en revanche directement applicable. Par conséquent, au regard des règles européennes, le projet de loi ne peut recopier ses dispositions. C'est la raison pour laquelle les dispositions directement applicables et qui se suffisent à elles-mêmes ne figurent pas dans le projet de loi : il en est ainsi des dispositions relatives au délégué à la protection des données ou de celles attachées aux droits des personnes concernées, qui pourront néanmoins être invoquées directement à compter du 25 mai 2018. Il faudra donc, en tout état de cause, lire cette nouvelle version de la loi de 1978 avec le règlement européen à portée de main, ce qui, je vous le concède, n'est pas toujours évident… Il nous reviendra de proposer, sur les sites officiels, notamment celui de la CNIL, des versions commodes, avec des liens hypertextes, afin que tout un chacun puisse s'y retrouver.

Mais le projet de loi qui vous est soumis ne constitue pas seulement un simple exercice de transposition de la réglementation européenne : le règlement européen prévoit plus d'une cinquantaine de marges de manœuvre qui autorisent les États membres à préciser certaines dispositions. La plupart de ces marges de manœuvre permettent de maintenir des dispositions qui existaient déjà dans notre droit national. D'autres, à l'inverse, peuvent être utilisées afin notamment de prendre en compte l'évolution technologique et sociétale que la loi de 1978 ne permet plus d'appréhender.

Le Gouvernement, conformément à la démarche de simplification des normes souhaitée par le Président de la République et à sa volonté d'éviter la surtransposition des textes européens, a fait le choix d'épouser la nouvelle philosophie du règlement et de supprimer la plupart des formalités préalables à la mise en œuvre des traitements.

Cependant, afin de ne pas affaiblir la protection des données à caractère personnel, et bien que ce ne soit exigé ni par le règlement ni par la directive, le Gouvernement a fait le choix de maintenir certaines formalités préalables pour le traitement des données les plus sensibles, par exemple pour les données biométriques nécessaires à l'identification ou au contrôle de l'identité des personnes, pour les données génétiques, ou encore pour les traitements utilisant le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR). Les traitements utilisant des données de santé font eux aussi

l'objet d'un régime protecteur et unifié. Enfin, dans le champ d'application de la directive, sont également maintenues les formalités préalables à la création de tout traitement mis en œuvre pour le compte de l'État.

Par ailleurs, un point important, qui retient tout naturellement votre attention, doit être précisé. Le règlement fixe à seize ans l'âge à partir duquel un mineur peut consentir à une offre directe de services de la société de l'information – autrement dit, pour parler clairement, accéder aux réseaux sociaux. Le Gouvernement a ici fait le choix de ne pas utiliser la marge de manœuvre prévue à l'article 8 du règlement, qui permet aux États membres d'abaisser ce seuil jusqu'à treize ans. Le projet de loi ne contenant aucune disposition sur l'âge du consentement, le règlement s'applique directement et l'âge limite reste fixé à seize ans.

Notre préoccupation commune est bien entendu de mieux protéger les mineurs, et la fixation d'un seuil est toujours un exercice délicat. On tente de saisir par une norme générale des cas éminemment particuliers, surtout lorsqu'il s'agit d'identifier ce que peut être le seuil de maturité d'un enfant ou d'un mineur. La France avait défendu le seuil de seize ans, en deçà duquel l'autorisation parentale sera nécessaire pour autoriser le traitement des données. Les autres pays de l'Union font des choix très divers. Nous avons souhaité maintenir notre position dans le cadre du projet de loi, mais j'ai bien conscience que ce point fait débat.

Il nous semble, en tout état de cause, que la mise en place d'une autorisation parentale, sans lourdeur procédurale excessive, doit être l'occasion de réinstaurer le dialogue au sein de la famille sur ces questions et permettre ainsi une meilleure connaissance par les parents des pratiques numériques de leurs enfants. Il s'agit également de prendre en considération la difficulté pour les adolescents de comprendre et de mesurer les conséquences de la diffusion de leurs données personnelles et les risques inhérents encourus, en termes de marchandisation des données personnelles à des tiers, de réputation en ligne. Je crois que nous sommes tous d'accord sur ces objectifs ; le débat nous permettra certainement de progresser.

Je voudrais enfin dissiper un certain nombre d'interrogations concernant l'habilitation que le Gouvernement sollicite dans le cadre du projet de loi. Le Gouvernement souhaite qu'en mai prochain, date limite de transposition de la directive, nous soyons prêts ; nous le serons. Pour cette raison, il a fait le choix d'un texte le plus resserré possible, qui ne remette pas sur la table l'ensemble de la loi de 1978, ce que le droit européen n'exige nullement.

L'objet de l'habilitation qui vous est demandée est de permettre une codification des modifications apportées à notre droit et à la loi fondatrice de 1978 par le projet de loi qui vous est soumis, afin d'offrir un cadre juridique lisible à chaque citoyen et acteur économique. Il ne s'agira aucunement de revenir sur les choix que le Parlement sera amené à faire lors de l'examen du projet de loi. Vous l'avez tous compris en lisant ce texte, l'accessibilité et l'intelligibilité du droit

requièrent une réécriture intégrale de la loi du 6 janvier 1978, pour qu'elle retrouve son ambition originelle : celle d'être un véritable code de la protection des données personnelles des Français. C'est le sens de cette habilitation, qui permettra d'adopter un plan clair, avec un titre I[er] rappelant les principes fondamentaux et les pouvoirs étendus de la CNIL, un titre II consacré au champ du RGPD, un titre III consacré à la directive et un titre IV consacré aux dispositifs hors du champ de l'UE.

L'ordonnance, qui sera édictée au plus tard à l'automne, sera donc de nature exclusivement légistique. Entre mai et la sortie de l'ordonnance, soyez par ailleurs assurés que tous les outils pédagogiques et de communication seront mis en place, avec la CNIL et les professionnels, au service des citoyens et des entreprises. Je suis d'ailleurs persuadée que nos débats auront aussi cette vertu pédagogique et qu'ils permettront d'écarter les inquiétudes les plus vives qui sont normales à l'occasion d'un tel changement de paradigme.

Pour conclure, je souhaite que chacun puisse mesurer la portée de cette réforme à l'aune non seulement du projet de loi qui vous est proposé mais, plus largement, des textes mis en œuvre par l'UE. L'exercice de transcription du droit européen présente toujours un caractère un peu contraint, mais le nouveau cadre adopté par l'Union pour la protection des données personnelles est, me semble-t-il, une magnifique réussite pour l'Europe et les citoyens de l'UE.

Mme Paula Forteza, rapporteure de la commission des Lois. « *L'informatique doit être au service de chaque citoyen. (...) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée* » : cette ambition exprimée à l'article 1[er] de la loi « Informatique et libertés » a fait de la France un pays précurseur en matière de protection des données personnelles depuis 1978. En effet, la France a été le premier pays européen à se doter du cadre juridique et institutionnel nécessaire à la mise en œuvre de cette politique. Mon premier souhait serait donc que nous puissions être à la hauteur de ces engagements tout au long de notre travail en commission et en séance.

Pour ce faire, il nous faudra en permanence garder à l'esprit la portée économique et sociale de ces textes. Les enjeux sont transversaux : en témoigne la présence parmi nous de collègues des commissions des Afaires européennes, des Affaires économiques et des Affaires sociales, que je salue. Si la perspective des dispositions que nous allons étudier est celle des libertés individuelles et de la protection des droits des personnes, nous devrons en évaluer les incidences de façon globale. Le Conseil d'État a appelé à mener une réflexion de société autour de l'interaction entre la protection des données personnelles et la politique numérique de la France au sens large ; je rejoins naturellement ces propos.

Les dispositions du paquet européen et du présent projet de loi constituent bel et bien un signal positif en termes de promotion de l'innovation. Ces textes tirent les conséquences des bouleversements technologiques survenus dans le traitement des données – citons par exemple le *cloud computing* ou l'internet des

objets – et du développement de son économie. Il fallait en effet changer de paradigme pour que la protection des données personnelles soit effective dans un contexte incertain où les avancées techniques sont toujours plus rapides que la capacité du législateur à en évaluer les conséquences. Il conviendrait de laisser des marges de manœuvre aux différents acteurs pour accomplir leurs missions et leurs activités : l'allégement des démarches administratives, la responsabilisation des acteurs, l'appel à des dispositifs de droit souple, l'homogénéisation des normes au niveau européen sont autant de bonnes nouvelles tant pour les entreprises que pour les citoyens et pour les organismes de contrôle. Il s'agit de construire les cadres de régulation de manière plus flexible, itérative et collaborative, de façon à ce qu'ils soient adaptés aux enjeux du numérique.

Ce seront aussi la portabilité des données, l'extraterritorialité des normes et le rôle accentué de la CNIL en tant qu'accompagnatrice des entreprises qui deviendront une source d'innovation en nivelant le terrain de jeux et en favorisant la concurrence loyale car – ne nous le cachons pas – tout se jouera sur la manière dont les entreprises se saisiront de cette nouvelle réglementation, en particulier les très petites entreprises (TPE) et les PME qui, pour la plupart, sont encore loin de la mise en conformité. La prise de conscience de ces difficultés sera la clef de voûte d'un dispositif qui permettra de transformer l'adaptation aux nouvelles dispositions en atouts économiques et d'en faire une véritable valeur ajoutée aux yeux non seulement des citoyens, mais aussi des consommateurs de biens et de services numériques. Cette nouvelle attractivité économique et juridique est une opportunité pour la France, qui pourra construire dans le cadre européen un modèle alternatif de croissance autour d'un numérique plus éthique, plus accessible, plus décentralisé que ne le sont actuellement le modèle américain ou le modèle chinois.

Mme la garde des Sceaux ayant déjà très bien présenté les textes européens, je me contenterai de rappeler brièvement les principaux apports du projet de loi du Gouvernement afin de bien en comprendre les enjeux.

Le RGPD est fondé sur un triple changement de la législation. Il s'agit tout d'abord d'un renforcement des droits des personnes lié à l'élargissement de la liste des données sensibles, à la protection accrue des mineurs et à de nouveaux droits tels que le droit à la portabilité des données, le droit à l'oubli ou encore le droit à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé. Ensuite, il s'agit de passer d'une logique de formalités préalables à une logique de conformité et de responsabilisation, comme l'a bien expliqué la ministre. Troisième objectif : le renforcement de la crédibilité de la régulation par l'extension de son périmètre d'application en dehors du territoire de l'UE, l'alourdissement des sanctions administratives et l'instauration d'un mécanisme de coopération entre autorités nationales de régulation afin d'assurer l'harmonisation des décisions au niveau européen. Par ailleurs, la directive constitue un instrument juridique permettant une harmonisation du niveau de protection au sein de l'UE en matière de traitement des données pénales.

Ces deux textes européens doivent être rendus applicables et transposés dans l'ensemble des États membres en mai 2018 au plus tard. Nous avons donc la responsabilité d'aboutir à l'adoption de ce projet de loi. Il s'agit d'adapter la loi « Informatique et libertés » du 6 janvier 1978 qui mérite, pour des raisons symboliques, d'être conservée et conformée aux dispositions européennes.

À cet égard, j'observe que le Gouvernement a fait le choix d'utiliser raisonnablement les marges de manœuvre offertes par le règlement et la directive lorsqu'elles semblent pertinentes, dans une démarche d'harmonisation européenne. Pour ma part, je vous proposerai d'aller plus loin que le Gouvernement dans l'utilisation de ces marges de manœuvre sur au moins deux points. Le premier a trait à l'action de groupe : je propose de permettre aux personnes ayant subi une violation des règles en vigueur de pouvoir obtenir réparation de leur préjudice matériel et moral par l'intermédiaire d'une association régulièrement agréée alors que l'action de groupe en matière de données personnelles est actuellement limitée à la seule constatation du manquement, contrairement à ce qui prévaut dans le domaine des discriminations et dans celui de l'environnement. Le second point concerne l'âge des mineurs : je propose d'abaisser à quinze ans l'âge à partir duquel un mineur peut consentir seul au traitement des données personnelles qui le concernent et prévoir le double consentement du mineur et de ses parents en dessous de cet âge.

Un travail sera également entrepris pour accentuer la lisibilité du texte qui, en l'état, est source de confusion pour la plupart des acteurs du secteur en raison des multiples renvois et superpositions des droits en vigueur. Nous avons d'ailleurs lancé un site sur lequel figure un dossier législatif en ligne comprenant les liens hypertexte et références qui permettent de naviguer plus facilement entre les différents textes, que vous pouvez consulter dès à présent à l'adresse suivante : https://donnees-personnelles.parlement-ouvert.fr.

Enfin, de nouvelles modifications pourraient être proposées à l'issue d'une séquence d'auditions complémentaires qui auront lieu entre l'examen en commission et la discussion en séance et auxquelles j'invite tous les commissaires à participer.

Pour le reste, je poserai à la garde des Sceaux quelques questions concernant des sujets qui me tiennent à cœur et sur lesquels j'ai souvent été interrogée lors des auditions que j'ai conduites. Tout d'abord, pouvez-vous nous présenter l'état d'esprit du Gouvernement concernant les modalités de contrôle des fichiers intéressant la sûreté de l'État, qui ne relèvent ni du règlement ni de la directive ? Vous paraît-il opportun de permettre à la CNIL d'effectuer un contrôle *a posteriori* sur leur fonctionnement, au-delà du contrôle ponctuel auquel elle procède par l'exercice du droit d'accès indirect et du contrôle *a priori* qu'exerce la Commission nationale de contrôle des techniques de renseignement (CNCTR) au stade de la mise en œuvre d'une technique de renseignement ?

Ensuite, s'agissant de l'extension de l'action de groupe en matière de protection des données personnelles, les auditions que j'ai conduites ont montré qu'il était nécessaire non seulement de l'étendre à la réparation du dommage causé par le manquement d'un responsable de traitement ou de son sous-traitant, mais aussi de trouver les moyens d'en assurer l'effectivité en prévoyant une prise en charge des frais de procédure engagés par les associations mandatées. Qu'en pensez-vous ? Autrement, quelle solution serait envisageable ?

Troisièmement, pouvez-vous nous rassurer au sujet des garanties apportées par le Gouvernement pour encadrer les décisions administratives individuelles prises sur le seul fondement d'un algorithme, dans le cadre de la marge de manœuvre offerte par le RGPD ? Plus particulièrement, pouvez-vous nous confirmer qu'il est toujours interdit d'adopter une décision de justice fondée sur le profilage d'un individu à partir d'un algorithme, tout comme les décisions administratives individuelles fondées sur des algorithmes auto-apprenants ?

Enfin, le projet de loi octroie de nombreuses missions nouvelles à la CNIL. Les ressources dont elle dispose vous semblent-elles suffisantes pour les mener à bien de façon efficace ? Sinon, quelles mesures prévoyez-vous à cet effet ?

Mme Albane Gaillot, rapporteure pour avis de la commission des Affaires sociales. Je tiens au préalable à remercier la commission des Lois pour son accueil chaleureux.

La commission des Affaires sociales s'est saisie pour avis des articles 7, 9 et 13 du projet de loi, sur lesquels elle a émis aujourd'hui un avis favorable. Je ne reviendrai pas sur la présentation de ces articles et concentrerai plutôt mon intervention sur les défis que représente le nouveau cadre juridique européen et national. Les responsables de traitement seront demain des acteurs déterminants du respect du nouveau cadre légal. L'appropriation des normes et leur impact économique ont été régulièrement abordés au cours des auditions que j'ai menées. Une certaine anxiété demeure et se nourrit parfois de la rédaction qui a été retenue. Sur ce point, il me semble nécessaire de faire œuvre de pédagogie.

Rappelons tout d'abord que la protection des données à caractère personnel n'est pas née avec le RGPD mais existe depuis 1978. En somme, nombreux sont les acteurs qui découvrent aujourd'hui qu'ils agissent en marge et parfois en infraction avec le droit en vigueur. Il importe donc de les accompagner dans l'application des normes européennes et nationales ; c'est à mon sens le premier défi.

Le deuxième défi concerne la CNIL. Elle a parfaitement anticipé les évolutions du RGPD en adoptant une doctrine d'emploi et en accompagnant les différents acteurs. Divers packs sectoriels ont ainsi été adoptés – le pack assurance, par exemple. La puissance publique doit quant à elle prendre toute sa

part pour faciliter la transformation de la CNIL vers ce rôle d'accompagnateur en renforçant ses capacités opérationnelles ; c'est un enjeu majeur.

Le dernier défi concerne les acteurs des données. J'entends par là les citoyens eux-mêmes, qui sont producteurs de données, ainsi que les responsables de traitement. Le principe de vigilance formulé par la CNIL dans sa synthèse du débat public qu'elle a animé dans le cadre de l'examen de la loi pour une République numérique nécessite que les citoyens s'approprient davantage la notion de consentement accordé à l'utilisation de leurs données personnelles, particulièrement de leurs données de santé. Un réel fossé existe entre le souci de protéger ces données et l'empressement quant au consentement accordé afin de profiter des outils de la vie quotidienne. J'ai notamment vu des internautes publier des informations relatives à leur santé – comme le NIR – sur les réseaux sociaux. Ce fossé doit être comblé. Dans un univers où tout a tendance à être numérisé, il nous faut donc entreprendre un ambitieux chantier de sensibilisation.

Ce dernier défi concerne aussi ceux qui seront appelés à participer au traitement de données à caractère personnel. S'agissant des données de santé, je pense aux professionnels de santé, aux industriels et aux organismes de recherche. Le recueil du consentement, le droit à l'information, le droit de rectification supposent de leur part une démarche éthique qui compte autant que la qualité des données recueillies. Cette démarche s'appliquerait aussi bien à la collecte des informations qu'au stade de leur traitement et de leur analyse. Je salue donc les orientations prises dans le texte qui visent à développer des labels et des certifications en appuyant l'idée d'un label éthique.

Il va de soi que tous ces enjeux n'appellent pas une réponse dans ce projet de loi. Il me semble cependant utile d'être attentifs à ces points si l'on souhaite que ce nouveau cadre réponde aux besoins sociétaux et à la demande de protection.

Mme Christine Hennion, rapporteure pour observations de la commission des Affaires européennes. Le projet de loi que nous examinons s'attache à adapter le droit national à un texte majeur, le RGPD, ainsi qu'à une directive adaptant la protection des données personnelles en matière pénale, formant ce que l'on appelle le « paquet données personnelles ».

L'idée de moderniser le cadre européen de protection des données personnelles est ancienne, puisque la Commission avait lancé une vaste consultation publique de deux ans, entre 2009 et 2011, pour faire évoluer le cadre juridique européen applicable aux données personnelles. Cela fait donc bientôt dix ans que les réflexions sont en cours, tandis que les négociations ont quant à elles duré quatre ans, de 2012 à 2016. La sensibilité de certaines données telles que les données de santé et la longueur des négociations expliquent le caractère tout à fait spécifique du RGPD, un règlement qui laisse plus d'une cinquantaine de marges de manœuvre aux États membres.

Les aspects que je souhaite évoquer relèvent précisément de ces marges de manœuvre nationales. Le Gouvernement a adopté une approche parcimonieuse en la matière et nous ne pouvons que le louer d'avoir privilégié l'harmonisation européenne la plus large possible. Cependant, j'estime que des marges d'amélioration existent sur plusieurs points.

Le premier point concerne l'âge du consentement au traitement des données à caractère personnel. Le règlement fixe cet âge à seize ans mais autorise les États membres à déroger à cette règle pour l'abaisser à treize ans. Il s'agit sans doute de l'une des marges de manœuvre qui seront les plus utilisées dans l'Union, pour plusieurs raisons. Tout d'abord, la limite fixée à seize ans n'est apparue qu'au cours des négociations, puisque la proposition initiale figurant dans le règlement était de treize ans. Un consensus européen peut donc être à nouveau trouvé sur cet âge-là.

Le traitement des données à caractère personnel des mineurs doit de toute façon se faire de telle sorte que le consentement soit donné en toute connaissance de cause, facilité par les informations données par les fournisseurs de services en ligne. Mais ne nous leurrons pas pour autant : les pratiques des adolescents dans le domaine numérique sont aujourd'hui telles que le recueil du consentement auprès des autorités parentales risque de n'être presque jamais mis en pratique. En tout état de cause, les réseaux sociaux ne seront pas en mesure de vérifier l'âge effectif des personnes inscrites sur leurs plateformes, et nous créerons ainsi en Europe des difficultés réglementaires dont les premières victimes seront nos TPE et PME. C'est pourquoi je souhaite que, dans ce projet de loi, l'âge à partir duquel un adolescent peut consentir au traitement de ses données personnelles soit abaissé à treize ans, en contrepartie d'un véritable projet d'éducation aux usages.

Le deuxième point complète le premier ; il vise à permettre aux utilisateurs de services en ligne dont les données personnelles sont traitées de pouvoir déclencher une action de groupe en responsabilité. Cette marge de manœuvre est aussi inscrite dans le règlement européen à l'article 80.1. Actuellement, le droit français issu notamment de la « loi Hamon » de 2014 et de la loi sur la justice du XXI^{e} siècle de 2016 ne permet que des actions de groupe en cessation de traitement, et non en réparation. La logique de responsabilisation des acteurs du traitement des données induite par le règlement voudrait pourtant que la violation de la vie privée des utilisateurs entraîne une juste indemnisation à leur égard. Je souhaite donc que le projet de loi soit amendé en ce sens.

Enfin, le RGPD a pour objet de renforcer considérablement le nombre et l'efficacité d'instruments dont les autorités nationales de contrôle – en l'occurrence la CNIL – disposent pour mieux accompagner les responsables de traitement, mais aussi pour sanctionner les contrevenants de manière plus drastique. Or je pense que le législateur devrait instituer, au croisement de ces deux logiques, la possibilité de mener des actions de médiation dans les phases précontentieuses entre professionnels ou entre particuliers et plateformes.

Telles sont les observations que je souhaitais formuler sur un projet de loi dont je tiens à rappeler la cohérence et la pertinence pour adapter la loi de 1978, qui fut un texte précurseur en la matière.

M. Philippe Gosselin, co-rapporteur d'application. Permettez-moi de nous replacer rapidement dans le contexte historique, à la veille de l'anniversaire que nous célébrerons jeudi comme il se doit avec la garde des Sceaux et la présidente de la CNIL à l'occasion des quarante ans de la CNIL et de la loi du 6 janvier 1978. Nous ne sommes plus dans le contexte des années 1974 où les fichiers du système SAFARI défrayaient la chronique et avaient incidemment permis de créer les premières autorités administratives indépendantes, appelées à former le « carré magique » de la transparence : la Commission des opérations de bourse, le Médiateur, la Commission d'accès aux documents administratifs et la CNIL – tel est l'héritage de cette belle période.

À la veille de célébrer le quarantième anniversaire de la CNIL, nous allons profondément modifier la loi de 1978 – pour de bonnes raisons, du reste, même s'il a fallu attendre ce texte assez longtemps. En mars 2012, j'avais commis une proposition de résolution européenne sur le sujet ; l'an dernier, Mme Anne-Yvonne Le Dain et moi-même avons essayé de préparer le terrain pour faciliter la transmission du relais d'une mandature à l'autre sans que nous ne nous trouvions acculés et obligés de légiférer dans la précipitation à la veille de l'entrée en application du RGPD le 25 mai ; c'est pourtant ce que nous constatons ce soir et je le regrette, même si je n'en incrimine pas particulièrement la garde des Sceaux, car je sais que ses services ont travaillé en bonne intelligence. Je déplore tout de même la précipitation dans laquelle nous nous trouvons. Alors que nous examinons en séance publique un texte sur la simplification, je constate qu'il reste des progrès à faire pour que cette simplification s'étende au deuxième sous-sol de cette noble maison et traverse les murs des différents ministères…

Quoi qu'il en soit, ce texte est d'une très grande importance et marque un profond changement de paradigme. La loi de 1978 nous avait habitués à une forme de « confort », à la fois pour les particuliers et pour les entreprises, sous la forme d'un système de déclarations préalables et d'autorisations. Demain, la charge de la preuve sera totalement inversée : il reviendra aux entreprises de démontrer qu'elles ont pris toutes les précautions nécessaires pour garantir le respect des données personnelles. Tout cela n'est pas simple à mettre en œuvre. La question de la protection des données personnelles des particuliers suscite aussi le débat : nous avons notamment soulevé le cas des mineurs, dont le consentement demeure un point important. Je constate d'ailleurs que le débat n'est pas clos entre les commissions et la majorité : le Gouvernement défendra l'âge de seize ans en se calant sur le règlement européen tandis que Mme la rapporteure proposera l'âge de quinze ans, comme je le ferai par amendement, par cohérence – car l'opposition sait parfois faire preuve de sagacité et a même certaines lueurs… La question de l'âge ne fait pas l'unanimité puisqu'il est également proposé de le fixer à treize ans ; nous verrons ce que donnera le débat, qui traverse aussi la société car les

parents, les jeunes et les adolescents peuvent eux aussi avoir des points de vue différents. Il est bon que ce débat puisse se poursuivre.

De même, il faut saisir l'occasion de ces textes pour renforcer les droits de nos concitoyens, affirmer la protection des mineurs et affirmer de nouveaux droits dans la continuité et la complémentarité avec la loi pour une République numérique, dite loi Lemaire, qui a été promulguée en 2016 et qui nous a quelque peu bousculés. Les débats ont régulièrement renvoyé à l'adaptation du règlement européen et de la directive, mais nous sommes restés en deçà de ces textes pour d'autres raisons.

En clair, la discussion doit se poursuivre, ce qui se fera de façon intéressante, je n'en doute pas. À ce stade, je vous assure de l'écoute attentive de l'opposition. Nous donnons volontiers acte au Gouvernement de sa volonté de ne pas surtransposer – encore faudra-t-il que les débats confirment cette volonté puisqu'il existe une cinquantaine de possibilités de surtransposition. Il ne faudrait pas que les positions françaises alourdissent trop les procédures. À titre personnel, je souhaite que nous préservions la singularité de la protection des données en France, qui est affirmée et réaffirmée avec force et conviction par la CNIL qui, ces dernières années, a su prendre une place très particulière en Europe en matière de protection des données, et qui permet sans doute de promouvoir à juste titre un modèle français voire européen auquel nous sommes attachés, excluant toute marchandisation poussée à l'extrême tout en réaffirmant la protection des données en général et de certaines données particulières comme les données de santé.

Mme la garde des Sceaux. Je vous remercie, Mme la rapporteure, pour vos propos ; comme vous, je pense qu'il est indispensable de bâtir une politique numérique ambitieuse pour la France. C'est une nécessité, et je sais que le dynamisme de mon collègue Mounir Mahjoubi y contribuera grandement.

De même, comme vous l'avez dit, il est nécessaire de mettre fortement l'accent sur les PME et les TPE, pour que ce processus très innovant leur permette de faire face à une concurrence loyale. Ce nouveau cadre juridique constitue un cercle vertueux dans lequel nous devons nous inscrire.

Je ne reviens pas sur les autres points de votre intervention, en particulier l'âge des mineurs, parce que nous y reviendrons au cours du débat. Je répondrai en revanche aux quatre questions que vous avez posées.

Vous m'avez tout d'abord interrogée sur l'état d'esprit du Gouvernement concernant les « fichiers de souveraineté ». Je rappelle que ces fichiers sont exclus du champ d'application du règlement et de la directive parce qu'ils ne relèvent pas du droit de l'UE. Si les fichiers pénaux entrent quant à eux dans le champ de la directive, et s'ils sont distincts des fichiers de souveraineté, ils feront bel et bien l'objet d'un contrôle de la CNIL en application de l'article 19 du présent projet de loi. En revanche, certains fichiers liés à la sûreté de l'État qui se trouvent hors du champ du droit de l'Union et qui sont dispensés de publication au *Journal Officiel*

font bien l'objet d'un contrôle *a posteriori* de la CNIL. C'est notamment le cas du fameux fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT), qui vise à lutter contre la radicalisation violente.

Rappelons donc que leur nombre est très réduit : leur liste est fixée à l'article 3 du décret du 15 mai 2007 et ne comporte qu'une dizaine de fichiers gérés par les services de renseignement et choisis parmi ceux qui ont été dispensés de publication. Ces dix fichiers dits « fichiers de souveraineté » ne peuvent faire l'objet de contrôles *a posteriori* par la CNIL, conformément au IV de l'article 44 de la loi de 1978. Qui plus est, ils font déjà l'objet de garanties propres à concilier de manière équilibrée la confidentialité des données qu'ils contiennent avec l'exigence d'un encadrement et d'un contrôle effectifs ; ces traitements de données ne peuvent avoir lieu que sur autorisation donnée après avis de la CNIL. Comme pour tout traitement de données, la CNIL est compétente dans le cadre de l'exercice du droit d'accès indirect prévu à l'article 41 de la loi de 1978. Le Conseil d'État est désormais compétent pour connaître des recours concernant la mise en œuvre du droit d'accès indirect. Ce dispositif issu de la loi sur le renseignement de 2015 permet de garantir qu'un juge indépendant se penchera sur le contenu de ces dix fichiers lorsqu'une personne s'inquiétera d'y figurer ou non, ce qui est une avancée considérable. La CNIL est systématiquement associée à la procédure en Conseil d'État.

Le Gouvernement considère que ces garanties sont suffisantes ; aller au-delà en conférant à la CNIL un pouvoir de contrôle *a posteriori* sur ces traitements risquerait de fragiliser considérablement leur alimentation et leur fonctionnement. D'une part, cela porterait atteinte au secret des modalités d'action des services de renseignement et, d'autre part, l'échange de renseignements entre les services français et ceux des autres États pourrait être freiné par la crainte des services étrangers que les renseignements confidentiels qu'ils partagent puissent être communiqués à des tiers. Nous semblons donc disposer pour nos services d'un modèle robuste, récent et efficace qui comporte des garanties réelles ; nous ne souhaitons pas prendre le risque de modifier ce dispositif à un moment où nos services sont en première ligne.

Vous m'avez également interrogée sur l'action de groupe. La loi de modernisation de la justice du XXI^{e} siècle du 18 novembre 2016, dite « J21 », a ouvert la possibilité d'actions de groupe en matière de protection des données, devant le juge judiciaire et devant le juge administratif. Ce recours sans mandat ouvert aux associations agréées et à celles existant depuis plus de cinq ans permet donc de solliciter du juge la cessation d'un manquement. En revanche, vous l'avez relevé, il n'y a pas d'action de groupe en réparation. C'est donc une différence par rapport aux autres actions de groupe prévues par la loi « J21 ». Par ailleurs, l'action de groupe créée par la loi du 17 mars 2014 relative à la consommation, dite « loi Hamon », première action de groupe instaurée, ne peut porter que sur la réparation des préjudices patrimoniaux qui résultent des dommages matériels subis par les consommateurs.

La loi « J21 » est récente. Le Gouvernement estime donc qu'il vaut mieux évaluer ce dispositif avant d'en proposer une modification. Cela étant, les arguments développés en faveur de l'action de groupe en réparation peuvent tout à fait être entendus. Sur ce point, le Gouvernement se montrera très ouvert et attentif, mais nous ne serons *a priori* pas favorables à un dispositif qui reviendrait sur celui de la loi « J21 » en permettant que les associations existant non plus depuis cinq ans, mais depuis trois ans puissent mener ces actions de groupe – c'est une garantie pour les personnes qui se lancent dans ces actions que d'avoir des interlocuteurs fiables. De même, les propositions visant à permettre à la CNIL de condamner les justiciables au remboursement des frais de procédure paraissent assez éloignées de nos principes de procédure civile. Pourquoi donner à une autorité administrative, aussi indépendante soit-elle, le pouvoir de condamner une partie à rembourser des frais de justice ? Ce mélange des genres semble difficile ; je n'en serai pas moins attentive, mesdames et messieurs les députés, aux propositions qui résulteront des débats.

Une de vos questions avait trait à la garantie du Gouvernement sur les décisions administratives individuelles fondées sur un algorithme. Je sais quelles craintes suscitent les algorithmes d'apprentissage, notamment ceux d'apprentissage profond, dont la capacité de traitement des informations se rapproche de celle de l'esprit humain. Mais pour ce qui est des décisions de justice, le projet de loi soumis ne modifie pas le premier alinéa de l'article 10 de la loi du 6 janvier 1978, qui pose le principe selon lequel « *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité* ». Nous n'irons donc pas plus loin, malgré les progrès qui peuvent résulter de ces algorithmes.

Enfin, les ressources aujourd'hui affectées à la CNIL lui permettent-elles d'assumer l'ensemble des missions qui sont les siennes en termes de communication, de pédagogie, de réflexion, de droit souple, de contrôle ? La question des moyens de la CNIL excède le champ de ce projet de loi et me semble plutôt relever de la discussion budgétaire. Je remarque toutefois que le budget de la CNIL a fortement augmenté depuis 2010, notamment les dépenses de personnel. L'enveloppe est ainsi passée d'un peu plus de 9 millions d'euros à 11 871 000 euros dernièrement, et, de 2010 à 2017, le plafond d'emplois est passé de 140 à 198. Les moyens alloués ont donc crû.

Le règlement européen crée de nouvelles missions pour la CNIL, mais il implique également une nouvelle philosophie dans la mise en œuvre des traitements de données. Au contrôle *a priori*, caractéristique du régime de déclaration et d'autorisation, est substitué un contrôle *a posteriori*. La réduction substantielle des formalités préalables à accomplir que le nouveau cadre juridique européen induit devrait permettre d'alléger la charge de travail de la CNIL, qui pourra se mobiliser davantage sur sa mission de contrôle. Nous n'en sommes pas moins attentifs à la question, car il est de l'intérêt de tous que la CNIL puisse

exercer ses missions de manière satisfaisante, notamment dans cette phase tout à fait essentielle de transition.

Mme Albane Gaillot a souligné les apports et les avancées du texte. Vous n'en appelez pas moins à notre vigilance sur un certain nombre de questions, madame la rapporteure pour avis, notamment celle des données de santé, bien entendu une préoccupation forte, que nous partageons. C'est la raison pour laquelle nous avons construit un système plus clair et unifié. Vous avez également insisté sur le statut dérogatoire de ces données, qui requièrent des garanties spécifiques ; c'est effectivement tout à fait important. Mme la rapporteure Forteza, qui s'est également penchée sur le problème, nous fera sur ce sujet des propositions que nous examinerons attentivement.

Madame la rapporteure pour observations Christine Hennion, vous avez insisté sur l'âge du consentement, comme M. Gosselin. Vous retenez plutôt l'âge de treize ans, tout comme Mme la présidente, et j'en prends note. De notre côté, Mme Forteza et moi-même envisageons plutôt un âge de quinze ans, quand d'autres proposent seize ans. La question est difficile et les réponses sont diverses, mais les pays européens, vous avez raison de le souligner, ont fait des choix extrêmement différents.

Sur l'action de groupe, j'ai déjà indiqué ma position.

Enfin, vous évoquez la possibilité d'actions de médiation dans des phases précontentieuses. La question mérite d'être traitée, mais je ne sais par qui, car ce n'est pas du ressort de la CNIL. En tout cas, votre proposition m'intéresse.

Non sans justesse, M. Gosselin parle de précipitation en même temps que de simplification. Il nous importait, monsieur le député, d'être prêts pour le 25 mai prochain. Les discussions ont été conduites depuis longtemps sur des textes complexes et des architectures compliquées, emboîtées. Aussi n'est-ce qu'aujourd'hui que nous vous présentons un texte. De nombreux pays européens – pas tous, certes – sont aujourd'hui dans la même situation. Bien sûr, je reconnais la complexité de la question et, nonobstant le site internet ouvert par Madame Forteza, qui nous donnera un accès numérique à l'ensemble des textes à notre disposition, la lecture n'en est pas des plus évidentes… C'est la raison pour laquelle une habilitation a été sollicitée aux fins de réécrire l'ensemble de manière très lisible. C'est tout à fait important.

Vous avez reconnu, monsieur le député, qu'il n'y avait pas de surtransposition excessive. Le Gouvernement y tient très fort, je le réaffirme devant vous. Soyez donc rassuré de ce point de vue.

Mme la présidente Yaël Braun-Pivet. Je propose que nous nous en tenions, pour la discussion générale, à un orateur par groupe. Chacun pourra ensuite s'exprimer lors de l'examen des nombreux amendements déposés.

M. Rémy Rebeyrotte. Madame la garde des Sceaux, chers collègues, il s'agit effectivement de mettre en œuvre dans le droit français ce paquet européen sur la protection des données personnelles : le règlement général sur la protection des données en matière civile et commerciale et la directive portant sur les infractions pénales. Le délai, certes, est très court, puisque tout doit être bouclé pour le mois de mai prochain.

La France a effectivement choisi de rester dans la logique de la loi du 6 janvier 1978 et de conserver la CNIL. Aussi évident qu'il puisse paraître, ce choix est un choix fort du Gouvernement, dans un cadre toutefois nouveau qui diffère de celui de la loi du 6 janvier 1978 et de ses révisions ultérieures. Le développement du numérique rend nécessaire une certaine fluidité, ce que permet le texte examiné : il fallait bien s'adapter à ces réalités.

Le principal changement est le remplacement du contrôle *a priori* et du régime de déclaration et d'autorisation par un contrôle *a posteriori*. L'exercice par la CNIL de ses missions s'en trouve évidemment modifié, mais il ressort de nos auditions et de nos rencontres avec la CNIL que celle-ci anticipe pour être au rendez-vous dès le mois de mai prochain. Autres changements, le projet de loi prévoit l'adaptation des services publics et des entreprises au droit européen et leur responsabilisation, sous-traitants compris, ce qui est une nouveauté ; il impose la production d'analyses d'impact, faites par des organismes certifiés, la désignation de délégués à la protection des données, une véritable formation sur ces questions et, conséquence logique du passage à un contrôle *a posteriori*, un sensible alourdissement des sanctions prévues qui pourront atteindre 4 % du chiffre d'affaires ou 20 millions d'euros.

Vous avez rappelé, madame la ministre, les quelques marges de manœuvre qui nous sont laissées. Vous avez notamment évoqué l'âge à partir duquel un mineur peut consentir à une offre directe de services de la société de l'information. Le texte initial le fixe à seize ans. Après consultation des acteurs, notre groupe soutient la proposition de notre rapporteure de l'abaisser à quinze ans. N'oublions pas la nécessité d'un accord des parents ni les sensibles efforts fournis depuis des années par les opérateurs pour prendre en compte la situation particulière des mineurs ; nous n'en souhaitons pas moins qu'ils s'emploient à améliorer la « charte d'entrée » et clarifient leur pédagogie avant de permettre l'accès à leurs services, à l'égard des jeunes mais aussi à l'égard des parents – les engagements pris au moment de consentir à une offre de services ne sont pas toujours très clairs. Il nous semble également important de maintenir une offre spécifiquement dédiée aux mineurs, qui les empêche d'accéder à certains profils sans autorisation ou, dans d'autres cas, permet de protéger leur propre profil. De tels dispositifs nous paraissent de nature à renforcer la protection des données personnelles des mineurs. Même si nous en connaissons les limites, un accompagnement de ces publics vers l'accès au numérique nous paraît possible.

Vous avez répondu sur l'action de groupe, madame la ministre, mais nous souhaitons aller au-delà de la constatation du manquement, vers la réparation, y compris sous la forme de dommages et intérêts lorsque cela s'impose.

Nous pensons que le texte réalise un certain équilibre entre innovation et protection dans les différents domaines, y compris la santé, la génétique ou la bioéthique, qu'il conviendra de ne pas trop remettre en cause : sans revenir sur la protection apportée par le droit européen, il faut permettre à l'innovation d'être au rendez-vous. Se pose également la question des algorithmes, des données nécessaires à la recherche ou des données liées au renseignement et à la sécurité. Là encore, la nécessité d'un équilibre entre protection et transparence doit être rappelée. Si le temps nous est compté, ces sujets n'en sont pas moins majeurs et nous invitons tous nos collègues à s'en emparer.

J'insiste un peu sur la question de l'âge de consentement. Que pensez-vous, madame la garde des Sceaux, de la solution des quinze ans et de la possibilité d'un renforcement de la protection des mineurs ?

Et qu'en est-il de l'accompagnement des entreprises ? La brièveté du délai impose de démultiplier l'information et d'être davantage présents à leurs côtés, pour les informer et leur permettre de se mettre aux normes.

Enfin, la question du droit à l'oubli, notamment *post mortem*, nous est souvent posée. Son importance s'est particulièrement manifestée lors des attentats. Qu'en est-il de la possibilité d'effacer les données relatives à une personne après le décès de celle-ci ?

M. Sébastien Huyghe. Je souscris totalement aux propos tenus tout à l'heure par notre collègue Philippe Gosselin. Il n'en sera pas surpris puisque j'étais son prédécesseur à la CNIL – en fait, nous avons même eu le plaisir de siéger ensemble. J'ajouterai simplement quelques points.

Le droit à la vie privée et à la protection des données personnelles est l'un des grands enjeux du XXI^{e} siècle, notamment eu égard au développement vertigineux du numérique et des réseaux sociaux. Il nous faut trouver une ligne de crête entre la protection de nos concitoyens et les intérêts de nos entreprises, qu'il s'agit de ne pas handicaper face à des concurrentes qui ne sont pas soumises aux mêmes règles.

Je veux rendre un hommage appuyé à ceux qui sont à l'origine de cette directive européenne, fruit de plus de dix ans d'un travail engagé par le « G29 » (groupe de travail de l'article 29 sur la protection des données), organe qui regroupe l'ensemble des CNIL européennes, longtemps présidées par l'ancien président de la CNIL, le sénateur du Nord Alex Türk, auquel je veux rendre hommage, et poursuivi par Mme Isabelle Falque-Pierrotin, actuelle présidente de la CNIL et également présidente du « G29 ».

Un certain nombre de dispositions du règlement, transposées par ce projet de loi, notamment l'alourdissement sensible des sanctions encourues, me satisfont particulièrement. La formation restreinte, organe de jugement de la CNIL, dont j'étais membre, infligeait parfois des amendes d'un montant ridicule au regard de la puissance économique des entreprises sanctionnées, telle Google. Une sanction doit être significative et dissuader de récidiver. Au demeurant, pour beaucoup d'entreprises, la pire sanction, c'est la publicité de la sanction… Je me souviens d'un grand organisme de formation dont la sanction avait été rendue publique. C'est cette publicité qui lui avait le plus nui… à tel point qu'il a fait des efforts considérables et est même devenu un modèle en la matière !

Je regrette, comme notre collègue Philippe Gosselin, le recours à la procédure accélérée mais, vous l'avez dit tout à l'heure, nous sommes pris par les délais. Il est vrai que l'année 2017, année électorale, ne se prêtait pas à l'examen d'un tel projet de loi par nos assemblées. Je n'en regrette pas moins amèrement que la réécriture d'un texte aussi fondamental que la loi « Informatique et libertés » se fasse par ordonnances. L'enjeu de la protection des données personnelles méritait un grand débat démocratique dans nos assemblées ; or vous vous apprêtez à nous en priver. C'est d'autant plus dommage que cela aurait été un moment de pédagogie vis-à-vis de nos concitoyens et l'occasion d'un choix de société : quelle société du numérique voulons-nous ? quelle protection de la vie privée et des données personnelles voulons-nous dans cette société ? Je vous conjure, madame la garde des Sceaux, d'user de votre influence pour que l'on revienne sur la décision de recourir aux ordonnances. Il est fondamental que nous nous emparions démocratiquement de ce sujet plutôt que de le laisser à de hauts fonctionnaires. Aussi grandes que soient leurs qualités, c'est aux élus du peuple qu'il revient de réécrire ce texte.

En tout état de cause, ces changements législatifs et réglementaires devront s'accompagner d'un important travail de pédagogie, notamment auprès de notre jeunesse, qui devra être engagé et amplifié par l'éducation nationale. Combien d'exemples avons-nous de ces jeunes qui viennent nous voir parce qu'ils sont poursuivis par des images d'eux-mêmes qu'ils avaient publiées sur les réseaux sociaux et qui ne les mettent pas en valeur, pour utiliser un doux euphémisme, au moment de rencontrer de potentiels employeurs !

M. Philippe Latombe. La protection des données à caractère personnel est un droit fondamental inscrit à l'article 8 de la Charte des droits fondamentaux de l'UE. La question préoccupe de plus en plus les citoyens, notamment sous l'angle du droit au respect de la vie privée. D'un autre côté, les données personnelles sont aujourd'hui des pièces essentielles des modèles économiques des entreprises, encore plus avec l'essor du numérique et du *big data*.

Le projet de loi soumis à notre examen vise à mettre la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés en conformité avec le droit européen à la suite de l'adoption, le 27 avril 2016, du « paquet européen de protection des données ». Il permettra l'application effective de textes qui

marquent – nous le pensons sincèrement – un progrès pour la protection des données personnelles des citoyens et la sécurité juridique des acteurs économiques.

Le « paquet européen de protection des données » se compose d'un règlement directement applicable dans les États membres à compter du 25 mai 2018, qui fixe le cadre général de protection des données, ainsi que d'une directive applicable aux fichiers de la sphère pénale, qui doit être transposée d'ici au mois de mai prochain. Mes collègues l'ont dit : nous déplorons vivement le délai qui nous est imparti pour adopter ce projet de loi. À l'avenir, il faudra anticiper.

Le RGPD est original en ce que, sur une cinquantaine de points, il prévoit des marges de manœuvre pour les États membres.

Le nouveau cadre juridique européen renforce les droits des personnes et responsabilise davantage l'ensemble des acteurs qui traitent des données personnelles, tout en leur fournissant des outils pour leur permettre de se mettre en conformité, par exemple un délégué à la protection des données, des analyses d'impact, etc. Il améliore la crédibilité de la régulation en renforçant la coopération entre les autorités de contrôle européennes et en instaurant des sanctions plus lourdes.

Bien que relativement technique, ce projet de loi n'en comporte pas moins de nombreux enjeux politiques. Ses dispositions visent une meilleure harmonisation et une plus grande cohérence entre tous les pays de l'UE afin qu'un organisme ne puisse plus choisir l'État dont le droit serait le plus avantageux pour lui. Le groupe du MODEM et apparentés salue le travail accompli par Mme la rapporteure Paula Forteza, la qualité des auditions auxquelles elle a procédé et celle des différents amendements déposés par ses soins. Le groupe votera ce texte dans son ensemble.

Nous n'en souhaitons pas moins aborder ce soir deux points sur lesquels nous avons déposé des amendements. Puisse une véritable discussion s'engager à l'occasion de leur examen, sans esprit partisan.

Il s'agit pour commencer de l'âge de la majorité numérique que nous proposons de fixer à quinze ans et non seize ans, comme la chancellerie le souhaite. Nos raisons tiennent autant à la cohérence législative qu'aux conseils et avis recueillis lors des auditions. Il s'agit ensuite de préserver le champ scolaire en le sanctuarisant. Comment parler de majorité numérique et autoriser l'exploitation de données issues de nos écoles et de nos collèges ? Nous aurons sans doute l'occasion d'en discuter, notamment aux côtés de nos collègues des groupes La France insoumise et Nouvelle Gauche, qui ont également déposé des amendements allant dans le même sens.

Enfin, nous aborderons avec bienveillance, en vue d'une discussion apolitique parce que d'intérêt général, les amendements sur le consentement, les algorithmes et les actions de groupe. Nous n'avons pas aujourd'hui de position

claire sur ces points, et nous souhaitons que les débats de ce soir nous permettent de nous positionner. À l'inverse, même si nous pensons que le sujet mérite d'être discuté et même si les États-Unis nous ont montré qu'il fallait en discuter, un amendement sur la neutralité du net n'a pas sa place dans ce texte ; c'est là une position plus ferme de notre part.

C'est ainsi avec un esprit d'ouverture que nous abordons l'examen de ce texte si important, qui affectera significativement le quotidien de nos concitoyens, et, en même temps, notre compétitivité dans la compétition mondiale du *big data*. Nous avons ce soir l'obligation de parvenir à une juste conciliation de ces exigences.

M. Stéphane Peu. Le groupe de la Gauche démocrate et républicaine votera ce projet de loi pour trois raisons principales. Premièrement, il va permettre de renforcer les moyens de protéger nos concitoyens contre les cyberattaques ; deuxièmement, certaines mesures concrètes, relatives au système de positionnement par satellites Galileo, vont permettre de renforcer la sécurité et la protection des citoyens, mais aussi de sortir de la dépendance à des systèmes de positionnement par satellites étrangers, dont le contrôle échappe aux pays européens ; troisièmement, la transposition de la directive va permettre de renforcer le contrôle de la circulation et du commerce des armes – cet aspect de la directive, initié par la France après les attentats de janvier 2015, va constituer un outil servant à sécuriser la vente d'armes à feu, mais aussi à lutter plus efficacement contre son trafic.

Cela dit, nous espérons que les débats feront évoluer la loi et l'enrichiront en un certain nombre de points sur lesquels le Conseil d'État et la CNIL ont indiqué qu'il convenait de faire preuve de vigilance. En la matière, nous reprenons à notre compte l'essentiel des observations de notre rapporteure, Mme Forteza.

Mme Marietta Karamanli. En écoutant les uns et les autres, on se rend compte que certaines préoccupations sont largement partagées. Pour ma part, madame la garde des Sceaux, j'aurai deux remarques à formuler.

D'une part, considérant qu'il a fallu dix ans de négociations, de travail parlementaire et de propositions émanant de la commission des Lois et de la commission des Affaires européennes, pour construire, avec le Parlement européen, un règlement et une directive, nous regrettons beaucoup que le Gouvernement ait décidé d'engager la procédure accélérée pour l'examen de ce projet de loi, même si nous pouvons comprendre que le calendrier électoral n'ait pas permis de le faire plus tôt : le seul fait que ce texte porte sur les droits et libertés imposait que l'on se donne le temps nécessaire à une vraie discussion.

D'autre part, comme l'a dit le Conseil d'État, « *l'étude d'impact n'éclaire, en dépit de son volume, qu'assez peu les choix stratégiques que le Gouvernement a pratiqués* », ce qui me conduit à vous demander des précisions sur trois points.

Premièrement, notre groupe souhaite savoir s'il a été procédé à une approche européenne et comparée. Le principe d'autorisation préalable concernant les traitements automatisés de données est remplacé par une auto-évaluation avec un contrôle *a posteriori* de la CNIL, dont le rôle va donc énormément évoluer. Le régime d'autorisation préalable n'est conservé que dans trois domaines : les données « sécurité sociale », les données biométriques et génétiques, et les données de santé. J'aimerais savoir si vous avez regardé ce que prévoient les autres législations européennes, et quels autres États européens ont fait le choix de passer du principe de l'autorisation préalable à celui de l'auto-évaluation. Par ailleurs, des études d'impact ont-elles été menées dans d'autres États, mettant en évidence les bénéfices et les inconvénients relatifs à la protection des secteurs d'intérêt public ?

Deuxièmement, comme l'a dit l'un de nos collègues, le projet de loi ne traite pas les données relatives à l'éducation et à la scolarité différemment de celles relatives aux autres domaines concernés, en dépit de l'avis exprimé par plusieurs spécialistes. M. Serge Abiteboul, informaticien, membre de l'Académie des sciences et du Conseil national du numérique, a ainsi déclaré : « *Le principe essentiel reste celui-ci : l'éducation nationale doit contrôler pleinement l'accès aux données et les mettre au service exclusif de l'éducation* ». Madame la garde des Sceaux, les données relatives à l'éducation et à la scolarité n'auraient-elles pas dû être considérées comme relevant d'un secteur sensible ?

Troisièmement, le projet de loi ne traite pas des droits des personnes à être informées de l'utilisation des traitements algorithmiques à leur endroit, notamment quand des décisions administratives pourraient leur être opposées. Ne pensez-vous pas que nous devrions prévoir que les règles relatives à l'utilisation des algorithmes, ainsi que les principaux effets attendus de leur utilisation, soient systématiquement communiqués aux administrés lorsqu'une décision leur est opposée sur la base d'un algorithme ?

Enfin, nous regrettons que des sujets dont nous avons longuement débattu au Parlement par le passé, notamment le droit à l'oubli ou la portabilité des données, ne soient pas traités par ce projet de loi – même s'ils le sont par le règlement.

Pour ce qui est de la réécriture de la loi de 1978, nous souhaitons qu'elle ne se fasse pas par ordonnances, mais puisse bénéficier de nos échanges en commission et en séance publique. Si je connais un certain nombre de hauts fonctionnaires travaillant dans différents ministères et dont les compétences ne sont plus à démontrer, je considère cependant qu'il faut toujours associer le Parlement à l'examen des textes portant sur des sujets aussi importants que celui-ci : il est en effet dommage de se passer de sa « *capacité d'étonnement* », jadis rappelée par Guy Carcassonne, qui lui permet souvent de porter un regard plus juste sur les textes et de les enrichir.

M. Bastien Lachaud. Madame la garde des Sceaux, je commencerai par exprimer le regret qu'inspirent au groupe de la France insoumise les conditions de préparation de ce projet de loi et la précipitation dans laquelle il est examiné, dénoncées tant par la CNIL que par le Conseil d'État. Nous déplorons aussi le choix du Gouvernement de légiférer par ordonnance sur des questions aussi importantes qui touchent aux droits et aux libertés numériques de l'ensemble de nos concitoyens.

En l'état, notre groupe ne pourra pas voter ce projet de loi, estimant que le Gouvernement a largement excédé ce qui était demandé par les textes européens, pour insuffler au texte une logique qui libéralise totalement le recours au fichage et qui affaiblit le rôle d'autorisation et de contrôle de l'État. Alors que les textes européens, notamment le règlement et la directive de 2016, avaient constitué des avancées positives en matière de droits, le Gouvernement profite de cette transposition pour réformer profondément le mode de contrôle de la CNIL sur les fichiers, en généralisant un régime de contrôle sous forme de supervision et en restreignant les déclarations préalables et autorisations à des domaines très limités.

En refusant de définir la notion de mission d'intérêt public, ou plutôt de lui donner un champ élargi, vous imposez une libéralisation pratiquement totale sur la totalité des fichiers. De même, le Gouvernement libéralise très largement la possibilité de développer le traitement des données à l'article 12, et le profilage administratif à l'article 14. Nous aurions préféré qu'il reste dans l'esprit initial du règlement et de la directive de 2016 en renforçant les droits et libertés numériques plutôt qu'en favorisant leur utilisation déraisonnée et marchande. Nous avons déposé plusieurs amendements visant à ce que les GAFA ne puissent continuer à échapper aux règles les concernant – en l'état actuel, les infractions ne sont sanctionnées que par des amendes d'un montant insignifiant pour ces sociétés –, et à renforcer les moyens de la CNIL et la transparence, en évitant les conflits d'intérêts. Enfin, nous proposons également des amendements relatifs à la neutralité du net ; cette question a toute sa place dans ce texte et nous l'estimons centrale pour la préservation des données personnelles. Tant que nous n'aurons pas l'assurance que toutes les questions que je viens d'évoquer ne sont pas réglées, nous ne pourrons voter ce texte.

Mme la garde des Sceaux. Je vais commencer par répondre à M. Rebeyrotte, qui a posé un certain nombre de questions, mais également fait le constat d'une prise de conscience générale, notamment par la CNIL, qui nous permet d'avancer.

Monsieur le député, vous avez fait part de votre position sur le consentement des mineurs ; je voudrais rappeler ce qui justifie la position du Gouvernement sur ce sujet. Comme je l'ai dit tout à l'heure, le Gouvernement a décidé de ne pas utiliser la marge de manœuvre dont il disposait, et de se référer à l'âge de 16 ans, proposé par le règlement.

Comme plusieurs d'entre vous l'ont souligné, il n'y a pas un consensus absolu entre les États membres de l'UE : la République tchèque, le Royaume-Uni et l'Irlande retiennent l'âge de 13 ans, l'Espagne pourrait retenir l'âge de 14 ans, la Grèce et la Croatie l'âge de 15 ans, l'Allemagne et le Luxembourg l'âge de 16 ans ; pour sa part, la France a toujours soutenu l'âge de 16 ans lors des négociations.

Nous savons la difficulté qu'il y a à établir un seuil, d'abord parce que cet exercice comporte toujours une part d'arbitraire ou de pari, surtout lorsqu'on travaille sur l'humain. En l'occurrence, il s'agit de saisir par une règle générale une multitude de cas particuliers : chaque enfant est différent, et mesurer la maturité de chacun d'eux, en prenant en compte l'environnement dans lequel ils vivent, est forcément délicat. Nous nous sommes fixé un objectif – partagé, me semble-t-il – consistant à prendre en compte la complexité des adolescents afin de comprendre et de mesurer au mieux quelles peuvent être les conséquences de la diffusion de leurs données personnelles sur les réseaux, et quels sont les risques en termes de marchandisation de ces données, d'exposition de l'intimité et de réputation en ligne – nous connaissons tous des exemples dramatiques de situations liées à ces problématiques.

Nous estimons également que recueillir le consentement des parents peut permettre, dans certains cas, de les responsabiliser, de restaurer le dialogue au sein de la famille et de mieux connaître les pratiques numériques de leurs enfants. Par ailleurs, même si les jeunes sont considérés comme matures à un âge de plus en plus précoce – y compris et même surtout en matière numérique –, on sait que les risques de fracture les plus importants se situent au cœur même de l'adolescence, vers 14 ou 15 ans, correspondant aux classes de quatrième, troisième ou seconde. C'est à cet âge critique que l'on constate le plus d'excès et de violences sur internet, et que les jeunes sont le plus enclins à répondre à des offres de services en ligne parfois douteuses.

Enfin, nous avons considéré que l'âge de 16 ans était un seuil déjà connu en droit français pour les mineurs : c'est celui qui est utilisé pour accomplir seuls les actes d'administration nécessaires à la création et à la gestion d'une entreprise individuelle à responsabilité limitée ; c'est également l'âge nécessaire pour participer à la constitution d'une association et être chargé de son administration ; pour choisir son médecin traitant ; pour établir un testament ; pour participer à la création d'une maison des lycéens ; pour assurer la direction ou la codirection de la publication d'un journal ; pour réclamer la nationalité française pour les mineurs étrangers, etc. C'est pourquoi nous n'avons pas souhaité utiliser la marge de manœuvre qui était proposée.

J'insiste sur le fait que le Gouvernement n'ignore pas que cette question fait débat ; les différentes propositions que vous avez évoquées en témoignent. Plusieurs amendements proposent un seuil de 15 ans qui correspond, lui aussi, à un âge retenu en droit français : c'est celui de la majorité sexuelle – ce terme est un peu impropre, mais c'est une autre question, qu'il nous sera peut-être donné

d'évoquer en d'autres occasions –, mais aussi celui à partir duquel les enfants peuvent s'opposer à ce que leurs parents accèdent à leurs données de santé. J'estime qu'il n'y a pas dans ce domaine de vérité absolue et je pense que le débat parlementaire va nous permettre de trancher cette question. En tout état de cause, il faudra un vrai travail pédagogique et la mise en place d'outils de sensibilisation pour encourager les acteurs du numérique à mieux protéger les mineurs. Je vous ai indiqué les raisons pour lesquelles nous avions choisi *a priori* l'âge de 16 ans, mais nous restons très ouverts sur cette question.

Vous avez également souhaité m'interroger, monsieur Rebeyrotte, sur les actions menées en direction des entreprises, notamment des PME ; il est en effet nécessaire de sensibiliser les entreprises, de les informer et de leur fournir des instruments pour les aider à prendre en compte cette nouvelle réglementation. Lors des négociations portant sur le règlement, la France s'est attachée à garantir la sécurité juridique et la transparence aux acteurs économiques, notamment aux PME – une préoccupation qui se traduit dans plusieurs dispositions du règlement, qui comporte des aménagements et des dérogations pour les PME : ainsi l'article 30 prévoit que la tenue d'un registre des activités de traitement ne s'applique pas aux entreprises de moins de 250 salariés. Le Gouvernement a traduit cette exigence en termes de dérogations et d'attentions apportées aux PME en proposant de modifier l'article 11 de la loi « Informatique et libertés ». Cette rédaction crée un nouvel environnement juridique grâce auquel la CNIL devra, entre autres, accompagner encore davantage les acteurs concernés, notamment les PME. Elle pourra désormais publier des lignes directrices – ce qui est évidemment important –, des recommandations ou des référentiels destinés à faciliter la mise en conformité avec le nouveau texte. Par ailleurs, le projet de loi supprime de très nombreuses formalités préalables. Cet ensemble de dispositions et ce choix revendiqué en faveur d'un droit souple, en faveur des PME, nous permettront, je l'espère, de faciliter la prise en compte rapide des nouvelles dispositions. J'ajoute que le ministère de la justice a mené des actions de sensibilisation très importantes, à travers des dossiers de presse et des rencontres avec des associations de petites et moyennes entreprises : c'est un sujet sur lequel nous sommes très sensibilisés et très attentifs.

Enfin, vous avez soulevé la question du droit à l'oubli *post mortem*. Le règlement ne s'applique pas aux données des personnes décédées, comme il est précisé aux considérants 27 et 158. Ce principe n'est pas exclusif du droit national, comme l'indique le considérant 27, qui affirme que « *les États membres peuvent prévoir des règles relatives au traitement des données à caractère personnel des personnes décédées* ». L'article 40-1 de la loi de 1978, modifié par la loi pour une République numérique de 2016, précise le régime qui est applicable nationalement aux personnes décédées en prévoyant que « *les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants* ». La direction des affaires civiles et du Sceau de la chancellerie rédige actuellement un décret en vue de créer un registre unique d'enregistrement des références des directives générales relatives à la conservation, à l'effacement et à la

communication des données à caractère personnel, même après le décès de la personne ; il est prévu que les directives générales puissent être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL. J'espère que ce texte répond à votre préoccupation ; je rappelle qu'il est également possible pour les héritiers, en cas de difficultés, de saisir les tribunaux pour sanctionner une atteinte qui serait portée aux droits de la personne décédée.

Monsieur Huyghe, je sais que vous connaissez extrêmement bien les questions que nous évoquons aujourd'hui. Vous avez fait le constat du développement vertigineux du numérique, souligné le rôle de la France dans l'élaboration des textes qui nous occupent, en rappelant le rôle joué par M. Alex Türk et Mme Falque-Pierrotin, qui ont successivement présidé le G29, et fait état de votre satisfaction quant à la puissance des sanctions dont pourra disposer la CNIL, et surtout quant à la publicité de ces sanctions, tout en regrettant la réécriture de l'ensemble de la loi de 1978 par ordonnance. Sur ce dernier point, je redis très simplement ce que j'ai déjà souligné dans mon propos introductif. Pour commencer, cette réécriture, prévue à l'article 20 du texte qui vous est soumis, est purement légistique ; avec tout le respect que je dois au Parlement, je ne sais si son intervention pourrait se traduire par un apport fondamental au contenu de la section I ou à l'intitulé de la section II, par exemple. Le débat au Parlement, nous l'avons maintenant, avec ce texte, puisque ce sont les décisions que nous prendrons maintenant qui se retrouveront dans la réécriture de la loi de 1978. Je vous rappelle ensuite que toute ordonnance est soumise à un projet de loi de ratification et que vous aurez donc la possibilité, comme c'est le cas actuellement avec l'ordonnance sur le droit des contrats, de débattre à nouveau d'un certain nombre de points. En tout état de cause, cette écriture qui se veut de pure légistique ne doit pas être perçue comme privant le Parlement d'un débat.

Monsieur Latombe, vous avez souhaité que l'âge de la majorité numérique soit porté à 15 ans : je me contenterai de réaffirmer devant vous que le Gouvernement est disposé à faire preuve d'ouverture lors du débat qui aura lieu sur ce point. Vous avez également abordé la question des algorithmes et des actions de groupe, points sur lesquels je crois avoir également répondu. Vous formez le vœu que le débat permette d'aboutir à de justes conciliations : je suis exactement dans le même état d'esprit et je suis persuadé que nous saurons trouver ces justes conciliations, pour reprendre votre expression, sur les différents points qui font débat.

Madame Karamanli, vous avez évoqué, entre autres points, la question des données personnelles et de l'éducation. J'entends votre préoccupation et je rappelle que le règlement européen et les protections qu'il institue s'appliquent pleinement au domaine de l'éducation. Comme vous, nous serons attentifs à cette question ainsi qu'à celle des algorithmes, très utilisés par l'éducation nationale – nous en avons un exemple récent avec l'application post-bac. Une convention a été conclue entre la CNIL et le ministère de l'éducation nationale le 10 mars 2016, qui porte sur les usages responsables et citoyens du numérique à l'école. Cette convention permet tout à la fois de concevoir des ressources pédagogiques en

matière de protection des données personnelles, ce qui est très important, ne serait-ce que par rapport au point que nous avons précédemment évoqué sur l'âge du consentement, de les mettre à disposition et d'organiser des actions de formation – tout cela grâce à un comité de pilotage chargé de suivre cette convention. S'il n'y a pas là matière à répondre à la question des algorithmes, cela peut fournir des outils pédagogiques de sensibilisation, et c'est un dossier sur lequel nous serons évidemment très attentifs.

Vous avez également évoqué l'approche européenne et comparée. Nous avons évidemment regardé ce qui se fait dans les autres pays de l'UE, et je dois dire que les marges de manœuvre ouvertes par le règlement traduisent souvent des préoccupations purement nationales, du moins est-ce ainsi que les choses m'apparaissent. C'est le cas notamment pour le NIR, qui est utilisé uniquement par la France ; c'est également le cas des données des églises, utilisées uniquement par la Pologne. Dans ces conditions, il me paraît difficile d'établir une comparaison fine, d'autant que, je l'ai dit tout à l'heure, tous les États membres n'ont pas encore établi leur nouvelle réglementation : les parlements nationaux travaillent actuellement à cette transcription du droit européen, et c'est seulement une fois que cette transcription aura été effectuée dans tous les pays que nous pourrons réellement établir un bilan.

Pour vous fournir un rapide état des lieux, je vous dirai que l'Allemagne a transposé partiellement – certains Länder n'ont pas terminé –, que l'Autriche a transposé, et que le Royaume-Uni, le Luxembourg, l'Espagne et les Pays-Bas ont déposé un projet de loi de ratification. Nous ne sommes donc pas tout à fait en retard et il sera intéressant de regarder, le moment venu, ce qu'ont fait les autres pays.

Enfin, vous regrettez que ne soient pas mentionnés le droit à l'oubli et la question de la portabilité des données, mais si ces points ne font pas l'objet de précisions, c'est qu'ils relèvent de dispositions de nature réglementaire.

M. Lachaud a exprimé ses regrets sur la précipitation dans laquelle, selon lui, nous examinons le texte, et sur la volonté du Gouvernement de légiférer par ordonnance. Il a également exprimé ses craintes d'une importante libéralisation des modalités de contrôle et de traitement des fichiers. Je reconnais que nous entendons inverser complètement la logique en vigueur puisque nous prévoyons tout à la fois de responsabiliser l'ensemble des acteurs et d'accroître les pouvoirs de contrôle de la CNIL – mais, de notre point de vue, il s'agit d'une logique beaucoup plus protectrice des citoyens. Nous nous engageons dans un bouleversement de nos procédures, certes, mais il n'y a pas lieu d'y voir une libéralisation complète des fichiers.

Je vous remercie, monsieur Peu, pour le soutien que vous apportez au texte. Vous évoquez des mesures concrètes pour renforcer la sécurité et la protection des citoyens et vous avez mentionné à juste titre le déploiement du système GALILEO qui, grâce au texte, verra d'une certaine manière sa légitimité

renforcée. Je retiens également vos considérations sur le contrôle et la vente des armes, ce qui m'avait échappé au premier abord. Vous avez raison d'appeler à la vigilance sur certains points que vous relevez dans l'avis du Conseil d'État, et que la discussion permettra d'améliorer, j'en suis certaine.

La Commission en vient à l'examen des articles du projet de loi, qu'elle poursuit lors des deuxième et troisième réunions du mercredi 24 janvier 2018.

EXAMEN DES ARTICLES

TITRE IER
DISPOSITIONS COMMUNES AU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 ET À LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016

CHAPITRE IER
Dispositions relatives à la Commission nationale de l'informatique et des libertés

Avant l'article 1er

La Commission ***adopte*** *l'amendement rédactionnel CL88 de la rapporteure, portant sur le titre du Chapitre Ier.*

Puis elle en vient à l'amendement CL5 de Mme Marietta Karamanli.

Mme Marietta Karamanli. Nous souhaitons préciser les exigences du règlement en matière de clarté et d'accessibilité des termes de la demande de consentement. De ce point de vue, un référentiel particulier destiné à orienter l'ergonomie des formulaires de demande de consentement doit être envisagé. Il s'agit d'éclairer tous les utilisateurs. Le présent amendement s'inspire des préconisations de la Commission nationale consultative des droits de l'homme (CNCDH).

Mme la rapporteure. Je partage votre préoccupation. Toutefois, sur la forme, l'alinéa que vous proposez d'ajouter à l'article 7 de la loi du 6 janvier 1978 devrait plutôt s'insérer à l'article 11 qui traite des missions de la CNIL. L'article 7 se borne à énumérer les conditions dans lesquelles les traitements des données personnelles sont autorisés.

Sur le fond, votre amendement est satisfait dans la mesure où la CNIL travaille déjà sur des référentiels destinés aux jeunes ou aux personnes pouvant rencontrer des difficultés de compréhension. Pour ces deux raisons, j'émets un avis défavorable.

Mme Marietta Karamanli. Reste qu'il est bon de le préciser tout de même…

La Commission ***rejette*** *l'amendement.*

Article 1er

(art. 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Missions de la Commission nationale de l'informatique et des libertés

Résumé du dispositif et effets principaux :

Le présent article a pour objet de compléter les missions dévolues à la CNIL en la chargeant de l'établissement et de la publication :

– des lignes directrices, recommandations ou référentiels destinés à accompagner les responsables de traitement et sous-traitants dans la mise en œuvre des nouvelles obligations qui leur sont faites ;

– des codes de conduite précisant ces obligations ;

– des règlements types assurant la sécurité des systèmes et régissant les traitements des données de santé.

La CNIL peut également soit procéder directement à la certification de personnes morales, de produits, de systèmes ou de procédures considérés conformes au règlement européen (1) et aux dispositions de la loi du 6 janvier 1978 (2), soit agréer des organismes certificateurs à cette fin.

Ces dispositions s'inscrivent dans la continuité de la démarche engagée par la CNIL au cours des dernières années de profonde refonte des outils et des procédures d'accompagnement des acteurs privés et publics en charge de traitements de données personnelles.

Par ailleurs, cette autorité pourra désormais être consultée par les présidents des deux assemblées parlementaires sur toute proposition de loi comportant des dispositions relatives à la protection ou au traitement de telles données.

Dispositions du règlement et de la directive concernées : articles 57 (considérant 117) du règlement et 46 de la directive.

Dernières modifications législatives intervenues :

L'article 59 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, anticipant pour partie l'application du règlement européen, a renforcé les missions et les pouvoirs de protection des données personnelles de la CNIL.

Modifications adoptées par la commission des Lois :

La Commission a modifié cet article de manière à prévoir :

– des dispositions en vue de mieux prendre en compte, au sein des missions de la CNIL, les besoins spécifiques des petites et moyennes entreprises ;

(1) Règlement 2016/679 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, directement applicable à compter du 25 mai 2018.

(2) Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

– un élargissement du recours aux règlements types pour les données biométriques et génétiques, du fait de leur sensibilité particulière ;

– l'extension aux commissions permanentes des assemblées parlementaires de la possibilité de saisir la CNIL sur une proposition de loi portant sur la protection des données personnelles.

Première autorité administrative indépendante, créée par la loi du 6 janvier 1978 précitée, la CNIL a pour principale mission d'assurer la protection des données personnelles et d'accompagner les responsables de traitements dans leur mise en conformité aux obligations qui leur sont faites par la loi.

Si le juge administratif intervient également, notamment à l'occasion de recours contre des actes administratifs autorisant des traitements de données, tout comme le juge judiciaire, notamment en matière pénale, l'importante activité de la CNIL et le renforcement progressif de ses pouvoirs et missions témoignent de la volonté du législateur de privilégier une approche administrative plutôt que judiciaire de la protection des données personnelles.

Par ailleurs, la CNIL est un membre actif du « groupe de l'article 29 », dit G29, institué par la directive 95/46/CE du 24 octobre 1995, qui regroupe les représentants des autorités nationales en charge de la protection de ces données afin de doter l'Union européenne d'un cadre d'échange, d'évolution et d'harmonisation des pratiques.

Elle a ainsi activement participé aux négociations ayant permis l'adoption du « paquet européen » sur les données personnelles en 2016 [(1)] et demeure une référence en termes de bonnes pratiques, notamment au titre des nouveaux outils d'accompagnement des acteurs privés et publics concernés mis en œuvre au cours des dernières années.

I. UN RENFORCEMENT PROGRESSIF DES MISSIONS DE LA CNIL

1. Les principales missions de la CNIL

Depuis la loi du 6 janvier 1978, une quinzaine de lois ont été adoptées de manière à adapter la législation nationale à la place croissante occupée par le numérique dans tous les domaines (économique, social, environnemental, recherche, médecine) et à la forte augmentation du nombre de données personnelles produites chaque année dans tous ces domaines d'activité.

La loi du 7 octobre 2016 pour une République numérique, inspirée des orientations du « paquet européen », constitue la dernière étape importante de cette consolidation progressive du cadre juridique national. Elle illustre également la

(1) Soit le règlement 2016/679 précité et la directive 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, qui doit être transposée au plus tard le 6 mai 2018.

volonté du législateur d'accompagner l'évolution des technologies numériques et leurs effets sur les droits des individus.

Parmi les principales mesures adoptées à cette occasion, le renforcement des pouvoirs et des missions de la CNIL illustre le souhait de garantir aux acteurs du numérique, comme aux citoyens, un cadre législatif et réglementaire adapté à leurs attentes.

La CNIL est chargée de **quatre missions principales**, mentionnées à l'article 11 de la loi du 6 janvier 1978, soit :

— **une mission générale d'information** de « *toutes les personnes concernées et* [de] *tous les responsables de traitements* [sur] *leurs droits et obligations* ». À ce titre, les demandes de renseignements (166 500 appels, 21 700 courriers et 12 200 requêtes électroniques en 2016) et les consultations de documents mis à disposition par la CNIL (2,6 millions de visiteurs du site) ne cessent de progresser d'année en année ;

— **une mission de contrôle** de la conformité des traitements de données personnelles aux dispositions de cette loi pouvant, le cas échéant, entraîner des **sanctions** en cas de non-respect des obligations prévues. À nouveau, ces contrôles sont en augmentation conformément au programme annuel que se fixe la CNIL (430 contrôles réalisés en 2016 ayant donné lieu à 82 mises en demeure et 13 sanctions) ;

— **une mission de conseil et d'accompagnement** des responsables de traitements en matière d'établissement des règles professionnelles relatives à la protection des données personnelles, notamment par la délivrance d'avis (145 avis ont été rendus en 2016) ou de labels (sur 136 demandes reçues, 97 ont été acceptées) ;

— **une mission de suivi de l'évolution des technologies de l'information** visant notamment à apprécier leurs conséquences sur l'exercice des droits et libertés mentionnés à l'article 1er de la loi aux termes duquel « [l]*'informatique (…) ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Ces missions permettent à la CNIL de développer un droit souple venant préciser la portée des règles de droit et sécuriser l'activité des acteurs concernés. Elle participe, en ce sens, à l'évolution de la norme nationale en matière de protection des données.

À ce titre, elle est également « *consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés* » et peut proposer des évolutions législatives ou réglementaires afin d'adapter la protection des libertés à l'évolution des procédés et techniques informatiques.

À la demande du Premier ministre, elle participe enfin à la préparation et à la définition de la position française dans les négociations internationales dans ce domaine, comme l'a illustré récemment son rôle dans les discussions européennes relatives à l'adoption du « paquet européen » sur les données personnelles.

La loi du 7 octobre 2016 a complété ces missions par :

— **l'élargissement des modalités de sa consultation** à toute disposition d'un projet de loi ou de décret relative au traitement ou à la protection des données personnelles. La consultation de la CNIL devient ainsi obligatoire même si l'objet principal du texte soumis à son avis ne porte pas exclusivement sur ces questions. Par ailleurs, alors que la publication de ses avis était conditionnée par la demande du président de l'une des commissions permanentes des assemblées parlementaires, elle devient systématique pour ceux pris sur un décret ou un arrêté conformément à une disposition législative ;

— **une réflexion sur les questions éthiques et sociétales soulevées par l'évolution des technologies numériques** [(1)]. La mission de la CNIL n'est ainsi plus d'assurer la seule protection des données personnelles mais bien de participer à l'étude plus générale des questions numériques. Cette évolution témoigne de la reconnaissance par le législateur du rôle de cette autorité et de sa légitimité acquise au cours des années. Dans son plan stratégique pour 2016-2018 [(2)], cette dernière se fixe d'ailleurs pour objectif de devenir « ***la référence pour le grand public en matière de numérique*** » ;

— **la promotion de l'utilisation des technologies protectrices de la vie privée**.

L'extension des missions de la CNIL constitue toutefois un défi pour cette autorité, dans un contexte d'évolution de la réglementation européenne et de nécessaire harmonisation des pratiques, mais également de demandes toujours plus nombreuses des acteurs publics et privés de précision sur les obligations qui leur sont faites.

La CNIL a ainsi été amenée à adapter ses méthodes et les outils d'accompagnement à sa disposition, dans le cadre de la constitution d'un droit souple, particulièrement adapté à l'évolution constante des technologies et des pratiques numériques.

---

(1) À ce titre, un premier rapport de la CNIL a été publié en décembre 2017 intitulé « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle *»* https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de.

(2) Plan stratégique de la CNIL 2016-2018 https://www.cnil.fr/fr/plan-strategique-2016-2018.

2. Le développement d'un droit souple

Comme le souligne le Conseil d'État dans son rapport relatif au droit souple [(1)], « *sans pouvoir ajouter aux dispositions législatives ou réglementaires,* [les instruments du droit souple] *définissent les critères qui guideront la décision de l'autorité.* ***Ils accroissent ainsi la prévisibilité de ces décisions pour les acteurs concernés.*** »

Par ailleurs, « *même si la CNIL ne pourrait fonder une sanction sur la seule méconnaissance d'une recommandation, l'article 45 de la loi du 6 janvier 1978 modifiée ne mentionnant que le non-respect "* des obligations découlant de la présente loi *", les responsables de traitement de données savent que les recommandations sont porteuses de l'interprétation de la loi effectuée par la CNIL et qu'ils ont donc tout intérêt à s'y conformer.* »

De manière à mieux accompagner les acteurs privés et publics chargés de traitements de données personnelles, la CNIL a ainsi mis à disposition :

— **des packs de conformité sectoriels** dans différents domaines [(2)] – construits avec les acteurs pertinents du secteur concerné – dont le double objectif est de sécuriser juridiquement les professionnels et de simplifier les formalités qui leur incombent. Ces packs donnent lieu, par exemple, à l'application de normes simplifiées, de procédures d'autorisations uniques, etc. ;

— **des labels** [(3)] pouvant être délivrés à des produits ou à des procédures assurant un haut niveau de protection des données personnelles ;

— **une évaluation des « *Binding corporate rules* »** (BCR) qui constituent les codes de bonne conduite adoptés par les entreprises et leurs sous-traitants en matière de transferts de données personnelles ;

— **une présentation des « Privacy Impact Assessment »,** catalogues de bonnes pratiques destinés à traiter les risques d'atteinte aux libertés et à la vie privée des personnes concernées par les traitements de données.

---

(1) Le droit souple*, Les rapports du Conseil d'État, 2013. Le Conseil d'État considère que le droit souple «* permet d'appréhender les phénomènes émergents qui se multiplient dans le monde contemporain, soit en raison d'évolutions technologiques, soit de mutations sociétales. Plus aisé à faire évoluer, ne formulant pas de règles générales insusceptibles de dérogation, il s'avère souvent plus adapté que le droit dur pour traiter de phénomènes qui ne sont pas tout à fait bien cernés, tout en préparant le recours ultérieur à ce dernier. Le droit souple a ainsi été utilisé en matière de prévention des conflits d'intérêts (chartes de déontologie des organismes de recherche et des agences sanitaires). Il joue un rôle prédominant dans le fonctionnement d'internet et est abondamment utilisé par la CNIL. *»*

(2) Quatre packs sont disponibles à la date de rédaction du présent rapport sur le site de la CNIL relatifs aux compteurs communicants, au logement social, au secteur assurantiel et aux véhicules connectés.

(3) Plusieurs types de labels sont proposés, notamment au titre de la gouvernance, des formations dispensées, d'un service de « coffre-fort numérique », de l'audit de traitements, etc. Par ailleurs, les acteurs concernés par le traitement des données personnelles peuvent soumettre à la CNIL des propositions de création de nouveaux labels.

Par ailleurs, la CNIL publie **des cadres de référence** permettant aux responsables de traitement de bénéficier de dispenses de déclaration ou de formalités allégées.

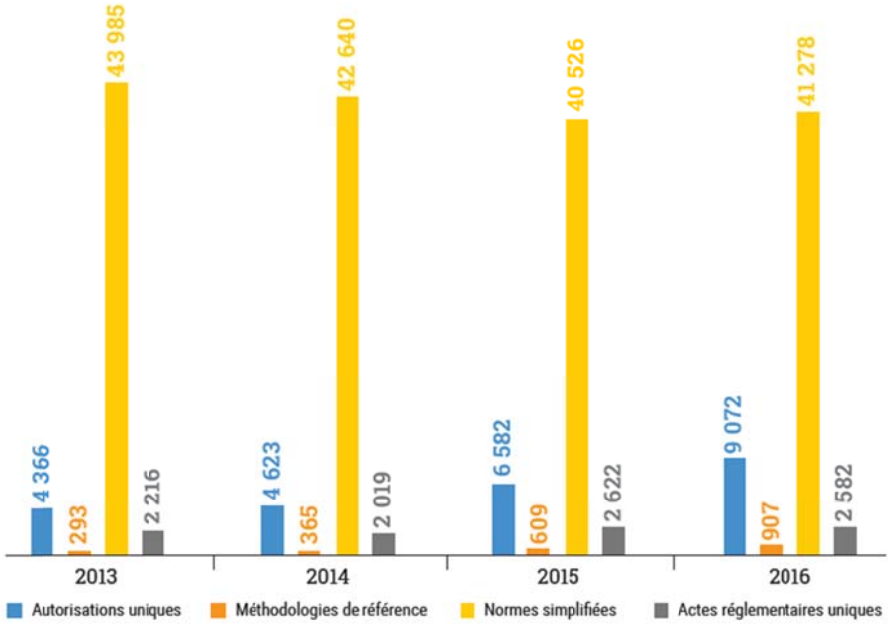
Le développement de ces outils de droit souple au cours des dernières années, **en concertation avec les acteurs publics et privés concernés**, s'inscrit dans une stratégie accentuée par la CNIL depuis 2012, dans un contexte européen favorable, de développement d'outils d'accompagnement et de prévention des risques, plutôt que de sanction.

L'une des quatre principales orientations retenues par le plan stratégique pour les années 2016-2018 consiste ainsi à « *ancrer la CNIL comme facilitateur de la transition numérique des acteurs publics et privés* ». À cette fin, cette autorité « *doit accompagner le développement de la confiance dans les services numériques, dans une logique de conformité et de respect des droits des personnes*. »

Cet objectif repose sur la proposition de nouveaux outils, comme des outils d'autoévaluation, la mise à disposition de labels, ainsi que sur le développement d'une doctrine plus adaptée et plus réactive aux besoins constatés sur le terrain.

Ces évolutions ont permis une simplification progressive des formalités administratives, tout en permettant l'homogénéisation et la diffusion des meilleures pratiques : les acteurs s'engagent à mieux respecter leurs obligations et en contrepartie, voient leur activité facilitée par des procédures adaptées.

L'ESSOR DES ENGAGEMENTS DE CONFORMITÉ DONNANT LIEU À DES PROCÉDURES SIMPLIFIÉES



Source : Rapport annuel de la CNIL pour l'année 2016, mars 2017.

II. LE DISPOSITIF PROPOSÉ

Le présent article modifie plusieurs dispositions de l'article 11 de la loi du 6 janvier 1978. Il tire en cela les conséquences des changements majeurs apportés par le paquet européen dans le rôle des régulateurs nationaux pour la protection des données personnelles.

1. Les dispositions du règlement européen

Alors que la directive du 24 octobre 1995 [(1)] faisait reposer en grande partie la protection des données personnelles sur un contrôle *a priori* exercé par le biais d'un système de formalités préalables contraignant, le paquet européen repose sur une logique de responsabilisation accrue des acteurs (« *accountability* ») et de contrôle *a posteriori*.

Ce changement de paradigme pose deux principes majeurs :

(1) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

— **la protection des données doit être assurée dès la conception** du service ou du produit (« *privacy by design* ») ;

— **les acteurs doivent se doter en interne de référents** (tels que le délégué à la protection des données) et **des outils** (registre des traitements, analyses d'impact sur la vie privée, etc.) nécessaires au contrôle du respect de cette obligation de protection.

Dans ce contexte, le rôle des autorités régulatrices est amené à sensiblement évoluer.

En premier lieu, le **considérant 117 du règlement** rappelle le principe selon lequel « *la mise en place d'autorités de contrôle dans les États membres**, habilitées à exercer leurs missions et leurs pouvoirs en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel*. »

En second lieu, le champ des missions de ces autorités tire les conséquences des modifications apportées à la protection des données personnelles. S'il reprend pour l'essentiel les quatre missions actuellement dévolues à la CNIL, il décline plus précisément celles relatives à l'information, au contrôle et à l'accompagnement des responsables de traitement dans leur démarche de conformité et des citoyens dans le respect de leurs droits.

Dans la majorité des cas, **les contrôles *a priori* seront supprimés**, tandis que l'accompagnement en faveur de la mise en conformité des acteurs sera fortement renforcé pour leur assurer une plus grande sécurité juridique, essentielle **notamment pour les PME et les TPE du secteur numérique**.

Le recours au droit souple est consacré comme un outil privilégié d'intervention des autorités de régulation pour définir précisément les obligations qui incomberont aux acteurs concernés.

À titre d'exemple, les autorités régulatrices pourront y recourir pour écarter des formalités superflues, conformément à **l'article 35 du règlement** qui prévoit que « *l'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.* » Elles disposent donc d'une marge d'appréciation importante permettant d'accompagner les responsables de traitement dans leur démarche de mise en conformité grâce à l'adaptation de leurs exigences au degré de risque identifié pour chaque type de traitement.

L'article 57 du règlement confie, par ailleurs, deux nouvelles missions aux autorités de contrôle, soit le recours à la certification des acteurs concernés, pour une durée maximale de trois ans renouvelable, et le rôle de conseil auprès du Parlement national.

L'article 46 de la directive prévoit, quant à lui, que les autorités régulatrices vérifient « *la licéité du traitement* […] *et informe la personne concernée dans un délai raisonnable de l'issue de la vérification* […] *ou des motifs ayant empêché sa réalisation* ».

2. Les dispositions de l'article 1er

Le rôle de la CNIL en matière de protection des données personnelles est réaffirmé en tant qu'« *autorité de contrôle nationale au sens et pour l'application du règlement européen* » (**alinéa 4**) (1).

Comme précédemment rappelé, ses missions sont profondément enrichies en vue de traduire le changement de paradigme souhaité par ce règlement. Au-delà des nécessaires coordinations légistiques qu'entraîne cette évolution (**alinéa 5**), la CNIL se voit ainsi reconnaître de nouvelles missions en matière d'accompagnement des acteurs concernés et de définition des risques d'atteinte aux libertés et aux droits fondamentaux emportés par les traitements de données personnelles.

a. La publication de lignes directrices et l'élaboration de codes de conduite

Dans le cadre de sa mission de contrôle du respect des dispositions de la loi du 6 janvier 1978, le rôle de l'autorité de régulation n'est plus de s'assurer de la prohibition de certains traitements et de l'autorisation ou de la déclaration préalable d'autres traitements, mais de définir les pratiques les plus adaptées à la prévention des risques que ces traitements pourraient entraîner.

Le régulateur devient ainsi un acteur essentiel de la définition des lignes directrices et des référentiels qui devront permettre aux responsables de traitement de s'inscrire dans le respect de la réglementation européenne et nationale, et d'harmoniser leurs pratiques.

L'alinéa 7 prévoit ainsi que la CNIL :

— établit et publie des **lignes directrices, recommandations ou référentiels** destinés à faciliter la mise en conformité des traitements des données personnelles et à procéder à l'évaluation préalable des risques par leurs responsables et leurs sous-traitants ;

— encourage l'élaboration de **codes de conduite** définissant les obligations qui incombent à ces derniers, **compte tenu du risque** inhérent à ce type de traitements pour les droits et libertés des personnes physiques. Pour mémoire, l'article 40 du règlement prévoit que ces codes devront prendre en compte « *la spécificité des différents secteurs de traitement et* [les] *besoins spécifiques des micro, petites et moyennes entreprises* » ;

---

(1) Cette insertion au début de l'article 11 a été considérée comme nécessaire par le Conseil d'État dans son avis n° 393836 du 7 décembre 2017 sur le présent projet de loi du 7 décembre 2017.

— homologue et publie les **méthodologies de référence** destinées à favoriser la conformité de ces traitements (cette dernière mission étant déjà prévue à l'article 54 de la loi du 6 janvier 1978) [(1)].

Dans son avis sur le présent projet de loi [(2)], la CNIL souligne « *le grand intérêt* » de ces instruments de droit souple auxquels elle recourt d'ores et déjà dans le cadre du changement de paradigme de sa mission de contrôle : « *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* ».

Ces mesures doivent également conduire à définir le cadre d'intervention de la CNIL pour les catégories de traitements les plus courantes et faciliter ainsi les démarches des acteurs concernés, en particulier les PME et les petites et moyennes industries (PMI).

En effet, comme le souligne le Gouvernement, « *les représentants des acteurs du numérique (associations, entreprises) ont indiqué ne pas se sentir encore prêts pour l'application du règlement et des nouvelles obligations qui leur incomberont. L'action combinée du Gouvernement et de la CNIL devra donc leur permettre de comprendre leurs droits et de mettre en œuvre les obligations prévues par les textes européens.* » [(3)]

b. Le traitement des données sensibles

L'alinéa 9 prévoit que la CNIL établit et publie **des règlements types** en vue d'assurer, d'une part, la sécurité des systèmes de traitement de données à caractère personnel et, d'autre part, de régir les traitements de données de santé.

À ce titre, sauf pour les traitements mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique**, elle peut prescrire des mesures techniques et organisationnelles supplémentaires pour le traitement des données biométriques, génétiques et de santé** conformément à l'article 9 du règlement européen [(4)] et des **garanties complémentaires en matière de traitement de données d'infraction** conformément à l'article 10 du même règlement [(5)]. Ces règlements sont alors contraignants pour les responsables de traitement concernés.

---

(1) Cet article prévoit ainsi que : « Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés. *»*

(2) Délibération n° 217-299 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 6 janvier 1978.

(3) Étude d'impact sur le présent article, annexée au projet de loi.

(4) Le 4 de cet article prévoit en effet que « les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. *»*

(5) Cet article prévoit, quant à lui, que le traitement de ces données particulières peut être autorisé par un État membre « qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées*. »*

c. La certification et l'agrément d'organismes certificateurs

L'alinéa 11 prévoit, par ailleurs, que la CNIL peut certifier des personnes, des produits, des systèmes de données ou des procédures de manière à reconnaître leur conformité au règlement européen et à la loi du 6 janvier 1978. Cette certification ne diminue pas la responsabilité des acteurs concernés, mais peut conforter leur image et leur accorder un avantage comparatif vis-à-vis de concurrents.

Elle peut également agréer des organismes certificateurs, sur la base de leur accréditation par l'instance nationale dédiée, soit le Comité français d'accréditation (COFRAC), à laquelle elle peut apporter des exigences supplémentaires.

d. L'identification des traitements risqués

L'alinéa 15 prévoit que la CNIL peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable, conformément à l'article 35 du règlement.

e. La consultation par les présidents des assemblées parlementaires

L'alinéa 17 propose de permettre aux présidents des deux assemblées parlementaires de saisir la CNIL sur des propositions de loi touchant à la question de la protection des données personnelles ou à leur traitement [(1)].

Cette extension des facultés de saisine de la CNIL n'avait pas été retenue dans le cadre de la loi du 7 octobre 2016. Elle est désormais explicitement prévue au c de l'article 57 du règlement : l'autorité de contrôle « *conseille, conformément au droit de l'État membre,* ***le parlement national****, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

f. Les observations en cas de litige

L'alinéa 19 prévoit que la CNIL peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement européen et de la présente loi.

Ces différentes mesures, qui complètent utilement les dispositions déjà en vigueur dans le droit national, doivent contribuer au renforcement de la protection des droits des personnes, mais également de « *l'attractivité économique et juridique de notre territoire vis-à-vis des opérateurs qui souhaiteraient s'y implanter.* » [(2)]

---

(1) À l'instar de la possibilité pour les présidents des assemblées de saisir le Conseil d'État d'une proposition de loi, avant son examen en commission, conformément à l'article 4 bis *de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.*

(2) Étude d'impact précitée.

Ces deux objectifs sont ainsi au cœur des missions de la CNIL, qui soutient résolument les avancées européennes venues en confirmer l'orientation.

3. La position de la Commission

La Commission a approuvé l'ensemble de cet article sous réserve de modifications rédactionnelles. Elle lui a toutefois apporté les modifications suivantes :

– le rôle de la CNIL en matière d'information des responsables de traitement sur les obligations qui leur sont faites est complété par une mission d'information personnalisée aux petites et moyennes entreprises. Votre rapporteure souligne, à cet égard, que la CNIL prend d'ores et déjà en compte les spécificités des différents secteurs économiques et de leurs acteurs en fonction notamment de leur taille et que les mêmes exigences ne sont pas attendues d'une grande entreprise ou d'une entreprise de taille plus modeste, sous réserve que la conformité aux règles de protection des données personnelles ait bien été recherchée ;

– la CNIL devra également, conformément aux dispositions du règlement européen, prendre en compte les besoins spécifiques des micro, petites et moyennes entreprises dans l'élaboration des procédures de certification et des codes de conduite ;

– ces codes de conduite devront, par ailleurs, prendre en considération les risques particuliers liés aux traitements de données portant sur des personnes mineures ;

– la possibilité pour la CNIL de recourir à des règlements types pour régir les traitements portant sur les données de santé a été étendue aux données biométriques et génétiques, qui présentent également une sensibilité particulière. Ces règlements devront être élaborés en concertation avec les organismes publics et privés représentatifs des acteurs concernés ;

– enfin, la possibilité pour les présidents de l'Assemblée nationale et du Sénat de saisir la CNIL sur une proposition de loi touchant à la protection des données personnelles est étendue aux commissions permanentes de ces assemblées.

*
* *

La Commission examine l'amendement CL13 de Mme Marietta Karamanli.

Mme Marietta Karamanli. Cet article ne mérite pas de figurer dans le texte. En proposant de le supprimer, nous entendons appeler l'attention de la représentation nationale sur le changement de paradigme évoqué au cours de la

discussion générale : le rôle désormais confié à la CNIL suscite de notre part une certaine inquiétude. Peut-être faudrait-il le réécrire différemment.

Mme la rapporteure. Nous avons déjà clairement souligné l'importance de ce changement de paradigme : c'est une des principales dispositions du texte. En outre, la question a été tranchée au niveau européen avec, depuis le début, le concours de la France. Avis défavorable.

La Commission ***rejette*** *l'amendement.*

Elle examine ensuite l'amendement CL239 de la rapporteure.

Mme la rapporteure. Cet amendement de précision vise à améliorer l'information des petites et moyennes entreprises, en particulier en ce qui concerne leur accompagnement par la CNIL.

Mme la garde des Sceaux. Le Gouvernement y est favorable.

M. Philippe Gosselin. L'amendement me va très bien. Reste qu'il pose la question des moyens de la CNIL dans la mesure où l'attribution d'une nouvelle compétence se traduira forcément par un travail supplémentaire qu'il ne sera sans doute pas possible d'assumer à périmètre constant.

La Commission ***adopte*** *l'amendement.*

Puis elle en vient à l'amendement CL240 de la rapporteure.

Mme la rapporteure. L'amendement CL240 précise que les responsables de traitement doivent respecter les obligations qui leur sont faites par la loi de 1978, mais également par tous les textes qui traitent de la protection des données personnelles.

La Commission ***adopte*** *l'amendement CL240*

Elle examine ensuite l'amendement CL21 de Mme Danièle Obono.

Mme Danièle Obono. Le texte prévoit que la mission principale de la CNIL, jusqu'à présent d'autorisation *a priori*, devient un contrôle *a posteriori* de supervision, ce qui revient à faire reposer la mission de garantie des droits fondamentaux, en matière numérique, en premier lieu sur les acteurs et les actrices du secteur. On peut considérer, comme l'a fait la garde des Sceaux, que cela les responsabilise, que l'on fait ainsi confiance aux entreprises numériques pour s'autoréguler et respecter les droits fondamentaux, même lorsque la violation de ces derniers pourrait générer un gain économique. Cette position défendue par la majorité nous semble insuffisante : on peut tout aussi bien considérer qu'elle revient à laisser le champ libre à ces entreprises et qu'elles parient sur le caractère fortement aléatoire du contrôle effectué par la CNIL – non par mauvaise volonté, mais tout simplement parce qu'elle ne dispose pas des moyens humains et techniques suffisants. Son budget s'élève en effet à 17 millions d'euros ; celui de

la FTC (Federal Trade Commission, Commission fédérale du commerce), aux États-Unis, qui a des missions équivalentes, est de 300 millions de dollars, soit presque vingt fois plus…

Au moment où l'on réforme cette autorité administrative en profondeur, il nous semble que l'augmentation de son budget reste très marginale et ne correspond pas aux nouvelles responsabilités qu'on entend lui donner. C'est pourquoi notre amendement CL21 vise à préciser les missions principales de la CNIL.

Mme la rapporteure. Vous partez du principe que l'autorisation préalable est plus protectrice qu'un contrôle en continu ; or ce n'est pas le cas. Il y a quelques années, les entreprises demandaient un avis de la CNIL et ensuite lâchaient prise – l'effort n'était pas continu –, alors que la responsabilisation des acteurs que nous souhaitons revient pour les entreprises à prouver qu'elles respectent constamment le droit en vigueur.

Nous avons donc un désaccord philosophique sur ce point. Avis défavorable.

M. Philippe Gosselin. La CNIL ne va pas tant assurer des contrôles qu'être éventuellement saisie d'un certain nombre de plaintes, ce qui en effet inverse la charge de la preuve ; la contrepartie de cette responsabilisation, c'est le montant des amendes qui seront prononcées : on passe d'un plafond de 150 000 euros à 4 % maximum du chiffre d'affaires consolidé, ce qui n'est pas rien puisque cela peut représenter plusieurs millions d'euros. Je ne vais pas défendre le texte à la place de la ministre ou de la rapporteure…

Mme la garde des Sceaux. Vous le faites pourtant très bien !

M. Philippe Gosselin.… mais il s'agit vraiment de nous conformer au règlement européen lui-même et, à ce stade, il est évidemment impossible, à moins de ne pas respecter du tout nos obligations, d'adopter un tel amendement.

La Commission ***rejette*** *l'amendement.*

Puis elle ***adopte*** *successivement les amendements rédactionnels CL89 et CL90 de la rapporteure.*

Elle en vient ensuite à l'amendement CL56 de M. Rémy Rebeyrotte.

M. Rémy Rebeyrotte. Nous souhaitons préciser que la CNIL encourage l'élaboration de codes de bonne conduite et notamment en ce qui concerne les mineurs afin de veiller au mieux à leur protection et au respect de leurs droits.

Mme la rapporteure. Voilà une précision bienvenue. Avis favorable.

La Commission ***adopte*** *l'amendement.*

Elle examine ensuite l'amendement CL241 de la rapporteure.

Mme la rapporteure. Le présent amendement vise à préciser que la CNIL prend en compte les spécificités des PME à l'occasion de l'élaboration des codes de bonne conduite.

Mme la garde des Sceaux. Je suis favorable à cet amendement qui répond aux préoccupations des PME.

*La Commission **adopte** l'amendement.*

*Puis elle **adopte** successivement les amendements CL242, de coordination, et CL243, de précision, de la rapporteure.*

Elle examine ensuite l'amendement CL23 de Mme Danièle Obono.

Mme Danièle Obono. Le présent amendement vise à élargir les compétences de la CNIL de la seule dimension de la sécurité du système à d'autres dimensions de protection des données : finalité, minimisation des données, respect des droits, notamment en matière d'ergonomie. Nous suivons en cela les recommandations exprimées par la CNIL elle-même dans son avis.

Mme la rapporteure. Nous allons proposer l'extension des règlements types à toutes les données les plus sensibles, portant sur la biométrie, la génétique et la santé, donc avis défavorable.

*La Commission **rejette** l'amendement.*

Elle en vient à l'amendement CL244 de la rapporteure.

Mme la rapporteure. Comme annoncé, cet amendement vise à élargir les règlements types aux données biométriques, génétiques et de santé.

Mme la garde des Sceaux. Le Gouvernement est favorable à cet amendement.

*La Commission **adopte** l'amendement.*

Elle examine ensuite l'amendement CL22 de M. Ugo Bernalicis.

Mme Danièle Obono. Nous souhaitons, concrètement, empêcher le pouvoir exécutif de créer un fichier dit « des honnêtes gens », qui concernerait plus de 20 millions de dossiers de demande de passeports biométriques et électroniques, et l'empêcher de créer un système national des données de santé, fichier géant et centralisé qui regroupe les informations de santé – feuille de soins, consultation, hospitalisations et achat de médicaments – de plus de 65 millions de Français et Françaises, cela sans contrôle de la CNIL. Or rappelons que dans son avis, celle-ci s'interroge sur la pertinence de l'exception que s'est octroyée l'État en la matière ; de même, nous estimons qu'il est difficile de comprendre à quelle

mission de service public pourrait bien correspondre ce type d'exemption dont bénéficierait l'État alors qu'il est ici question de la protection de données particulièrement sensibles.

Mme la rapporteure. Il y a exception dans ce cas du fait de la demande d'autorisation préalable prévue à l'article 9. Avis défavorable.

*La Commission **rejette** l'amendement.*

*Puis elle **adopte** successivement les amendements rédactionnels CL245, CL91 et CL92 de la rapporteure.*

Elle en vient à l'amendement CL246 de la rapporteure.

Mme la rapporteure. Il s'agit de prendre en compte les besoins spécifiques des PME, cette fois-ci dans la démarche de certification de la CNIL.

*La Commission **adopte** l'amendement.*

*Puis elle **adopte** successivement les amendements CL93, de précision, CL94 et CL96, rédactionnels, tous trois de la rapporteure.*

Elle examine ensuite l'amendement CL264 de la rapporteure.

Mme la rapporteure. Le projet de loi prévoit que la CNIL puisse être saisie par les présidents des deux chambres parlementaires. Nous souhaitons que les commissions compétentes de l'Assemblée et du Sénat puissent en faire autant.

Mme Marietta Karamanli. C'est un très bon amendement.

*La Commission **adopte** l'amendement.*

Puis elle en vient à l'amendement CL24 de Mme Danièle Obono.

Mme Danièle Obono. L'amendement CL24 s'inscrit dans la logique de l'article qui prévoit une saisine de la CNIL sur les propositions de loi concernant son domaine de compétence. Nous considérons cependant, à l'exemple de ce qui a été fait en matière de saisine du Conseil constitutionnel, qu'il serait important d'élargir cette possibilité de saisine aux parlementaires de l'opposition afin de permettre un plus haut degré de garantie des libertés fondamentales.

Mme la rapporteure. Votre proposition va un peu trop loin : la CNIL n'aura pas les moyens de répondre à la saisine de chaque député ou sénateur. Ce que prévoit l'amendement CL264 que nous venons de voter nous paraît un bon équilibre. Avis défavorable.

*La Commission **rejette** l'amendement.*

Elle examine ensuite, en discussion commune, l'amendement CL57 de M. Rémy Rebeyrotte, et les amendements identiques CL65 de M. Philippe Gosselin et CL73 de Mme Constance Le Grip.

M. Rémy Rebeyrotte. Nous proposons, après le mot « postes », de rédiger ainsi la fin de l'avant-dernier alinéa : « *ou toute autre autorité administrative indépendante ou organisme public en lien avec ses missions, de toute question relevant de leurs compétences*. » Le but est d'élargir le champ de la saisine.

Mme la rapporteure. Votre amendement CL57 est satisfait : la loi du 20 janvier 2017 prévoit déjà que la CNIL peut être consultée par différentes autorités indépendantes. Je m'en remets donc à la sagesse de la commission.

Mme la garde des Sceaux. C'est avec regret, monsieur le député, que je demande le retrait de votre amendement pour les raisons que vient d'invoquer la rapporteure : il nous semble aussi que votre amendement est satisfait par l'article 15 de la loi du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes. La loi de 1978 prévoit déjà que la CNIL peut saisir pour avis l'Autorité de régulation des communications électroniques et des postes (ARCEP). Désormais, avec la loi susmentionnée du 20 janvier 2017, elle peut saisir toute autre autorité administrative indépendante. Par ailleurs, votre amendement comme les deux suivants – CL65 et CL73 – sont insuffisamment précis, de mon point de vue, quant aux acteurs que la CNIL pourrait saisir pour lui apporter une expertise dans ses missions : on évoque des organismes publics dans un cas, une institution intéressée dans un autre, des autorités ou des institutions nationales enfin…

M. Rémy Rebeyrotte. Je retire mon amendement.

M. Philippe Gosselin. Bien sûr, la réforme du statut des autorités administratives indépendantes permet à la CNIL de saisir d'autres autorités administratives indépendantes. Mais l'objet est ici d'aller plus loin en incluant « toute autre autorité ou institution ». Les termes ne sont peut-être pas suffisamment précis, mais nous entendons signifier que la CNIL ne doit pas évoluer dans un environnement uniquement constitué de l'ARCEP ou de la Commission d'accès aux documents administratifs (CADA) – laquelle siège d'ailleurs au sein du collège de la CNIL ; je pense également à la Commission supérieure du numérique et des postes (CSNP).

Si la formulation est sans doute à revoir, j'y insiste, nous souhaiterions, par le biais de l'amendement CL65 qu'on pourrait dès lors considérer comme un amendement d'appel, connaître votre point de vue sur la possibilité d'élargir la saisine de la CNIL à d'autres instances que celles d'ores et déjà prévues.

Mme Constance Le Grip. Dans la droite ligne des propos qui viennent d'être tenus par nos deux collègues, je souhaite que la loi permette à la CNIL de saisir pour avis toute autre autorité ou institution intéressée par l'accomplissement

de ses missions, comme le propose mon amendement CL73. Je vous entends bien, madame la garde des Sceaux ; peut-être pourrions-nous travailler de conserve sur une rédaction susceptible de recueillir l'assentiment général – nous y sommes pour notre part tout à fait disposés.

M. Philippe Latombe. Il serait bon en effet de trouver, d'ici à l'examen du texte en séance, une formulation claire et qui, pour répondre au vœu de la garde des Sceaux, soit juridiquement sûre.

Mme la garde des Sceaux. Je suis tout à fait d'accord avec la proposition de M. Latombe : je demande, j'y insiste, le retrait de ces amendements et je suis favorable à ce que nous en retravaillions le texte d'ici à la discussion en séance.

Mme la présidente Yaël Braun-Pivet. Monsieur Gosselin, madame Le Grip, retirez-vous vos amendements ?

M. Philippe Gosselin. Je n'ai aucune difficulté à retirer mon amendement compte tenu de l'engagement pris à présenter un amendement en séance.

Mme Constance Le Grip. Je retire également le mien.

Les amendements CL57, CL65 et CL73 sont ***retirés****.*

La Commission ***adopte*** *l'article 1er* ***modifié****.*

Après l'article 1er

La Commission examine l'amendement CL25 de Mme Danièle Obono.

Mme Danièle Obono. Un des plus grands défis de la révolution numérique est selon nous qu'elle profite à tous et à toutes dans des conditions équivalentes. Par exemple, dans la vie de tous les jours, il faut savoir ce que signifie la mise à disposition de données personnelles collectées en masse, par exemple quand on souscrit à une carte de réduction avec avantages d'un hypermarché. La fracture numérique aggrave souvent les fractures géographique et sociale existantes ; pour certaines personnes, elle se traduit très concrètement par l'impossibilité d'accéder à leurs droits puisqu'elles ne comprennent pas certaines données apparaissant sur leur écran. Or les démarches auprès des services publics sont de plus en plus dématérialisées.

Le numérique est une nouvelle langue et on ne peut pas accepter qu'elle ne soit pas parlée par toute la population alors même que sa maîtrise en est de plus en plus supposée, voire exigée dans la vie sociale par les employeurs et employeuses et par l'État. Cela fait partie, selon nous, des missions étatiques essentielles en matière d'éducation. C'est pourquoi notre amendement CL25 donne la possibilité, à titre expérimental, aux départements, universités, académies et rectorats qui le souhaitent, de bénéficier de la compétence de la CNIL dans l'information du

public ou des élèves sur des enjeux liés aux droits et aux libertés numériques, aux moyens de se prémunir contre de possibles atteintes à ces droits et libertés.

Mme la rapporteure. Je partage vos considérations : l'éducation au numérique est pour les individus une clef déterminante en termes d'accessibilité, de capacité d'action, mais elle devrait plutôt être intégrée dans le cursus officiel de l'éducation nationale ou de formations proposées ou soutenues par l'État ; la CNIL interviendrait alors en soutien en proposant des contenus de formation. On ne saurait en effet lui confier une mission supplémentaire alors que nous savons qu'elle n'a pas encore les moyens d'assurer ses nouvelles fonctions.

M. Philippe Gosselin. Sans que la loi lui confie expressément ce type de mission, la CNIL a d'ores et déjà réalisé des opérations d'information avec des quotidiens, des revues, des magazines, etc, à destination de la jeunesse afin de faciliter cette appropriation. Cette action pédagogique existe déjà.

*La Commission **rejette** l'amendement.*

Article 1er bis (nouveau)
(art. 4 *bis* de l'ordonnance n° 58-1100 du 17 novembre 1958
relative au fonctionnement des assemblées parlementaires)
Saisine de la CNIL par les présidents des assemblées parlementaires

Résumé du dispositif et effets principaux :

Cet article inscrit, par coordination avec les dispositions prévues à l'article 1er, la possibilité pour le président d'une assemblée parlementaire de saisir la CNIL dans l'ordonnance n° 58‑1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

Dernières modifications législatives intervenues :

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a complété les missions de la CNIL en prévoyant l'élargissement des modalités de sa consultation à toute disposition d'un projet de loi ou de décret relative au traitement ou à la protection des données personnelles.

*
* *

*La Commission **adopte** l'amendement de coordination CL247 de la rapporteure. L'article 1er* bis *est ainsi rédigé.*

Article 2

(art. 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Qualification des personnalités désignées par le Parlement

Résumé du dispositif et effets principaux :

Le présent article aligne les conditions de nomination par le Parlement de deux personnalités qualifiées comme membres de la CNIL sur celles prévues pour les trois personnalités qualifiées nommées par le Gouvernement.

Elles devront ainsi disposer de compétences en matière de numérique ou **de protection des libertés individuelles**.

Dernières modifications législatives intervenues :

L'article 25 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a ajouté aux 17 membres composant la CNIL un représentant de la commission d'accès aux documents administratifs (CADA). Par ailleurs, pour les cinq personnalités qualifiées désignées par le Gouvernement et le Parlement, il a substitué à l'obligation d'une connaissance en informatique celle d'une connaissance du numérique, dont la portée est plus large et plus représentative de l'évolution des nouvelles technologies.

Modifications adoptées par la commission des Lois :

La Commission a adopté une disposition visant à rendre cumulatives les compétences exigées des cinq personnalités qualifiées membres de la CNIL. Ces dernières devront ainsi disposer de compétences en matière numérique et en matière de protection des libertés individuelles.

La composition de la CNIL, prévue par l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, doit permettre de garantir l'indépendance de cette autorité administrative. Ses membres ne peuvent ainsi recevoir d'instruction d'aucune autre autorité.

Depuis les modifications introduites par la loi du 7 octobre 2016 précitée, elle regroupe dix-huit membres nommés pour cinq ans ou pour la durée de leur mandat [(1)], soit :

— deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste ;

— deux membres du Conseil économique, social et environnemental ;

(1) Auxquels s'ajoutent le Défenseur des droits ou son représentant qui dispose d'une voix consultative, ainsi que le Commissaire du Gouvernement, désigné par le Premier ministre, qui siège auprès de la commission et qui peut être assisté de commissaires-adjoints.

— deux membres ou anciens membres du Conseil d'État ;

— deux membres ou anciens membres de la Cour de cassation ;

— deux membres ou anciens membres de la Cour des comptes ;

— le président de la CADA ou son représentant ;

— trois personnalités qualifiées **pour leur connaissance du numérique ou des questions touchant aux libertés individuelles**, nommées par décret ;

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

Cette distinction entre les compétences des différentes personnalités qualifiées participant à sa composition n'étant pas justifiée, le présent article propose de les aligner sur celles des personnalités nommées par décret.

Lors de l'examen de cet article, la commission des Lois a toutefois souhaité renforcer la légitimité des personnalités qualifiées nommées au sein de la CNIL en rendant cumulatives les compétences qui leur sont demandées en matière de connaissance du numérique et de protection des libertés individuelles.

*

* *

La Commission examine trois amendements identiques CL248 de la rapporteure, CL18 de M. Sébastien Huyghe et CL60 de M. Philippe Gosselin.

Mme la rapporteure. Je me réjouis qu'un consensus semble se dégager sur cet article. Les cinq personnalités qualifiées nommées membres de la CNIL doivent disposer tout à la fois de compétences numériques et de compétences touchant aux libertés individuelles, et non des unes ou des autres.

M. Sébastien Huyghe. Il était en effet de tradition qu'on demande aux personnalités qualifiées soit des compétences numériques soit des compétences sur les libertés individuelles. Du fait de la complexification de la matière traitée, il est devenu indispensable que les personnalités qualifiées nommées cumulent ces deux types de compétences. Il convient en effet d'élever le niveau d'exigence.

M. Philippe Gosselin. Il me semble effectivement indispensable que les personnalités qualifiées aient le même statut, et donc des compétences dans les deux domaines.

Mme la garde des Sceaux. J'émets un avis favorable à cette proposition.

Mme la présidente Yaël Braun-Pivet. Ces amendements identiques réécrivant l'ensemble de l'article 2, leur adoption rendra les amendements suivants sans objet.

M. Philippe Gosselin. En effet. Étant l'auteur de l'amendement CL66, j'en profite pour insister sur la nécessité à mes yeux de la double qualification des personnalités compte tenu de la complexité des données qu'elles auront à traiter.

Mme Danièle Obono. Notre amendement CL26 visait quant à lui à renforcer l'indépendance de la CNIL en rendant plus transparentes les conditions de nomination et en conditionnant celles-ci à des critères de compétence, ce qui n'est pas tout à fait le cas aujourd'hui. Nous proposions en outre la création d'un jury paritaire composé de membres d'organisations non gouvernementales (ONG), d'experts et expertes de la société civile, de citoyennes et de citoyens volontaires, tirés au sort et de membres de l'Assemblée nationale et du Sénat. Le but était de renforcer l'indépendance et de consolider le statut de la CNIL, amenée à devenir une institution cruciale dans la transition numérique.

Mme la rapporteure. Ces dispositions auraient été quelque peu complexes et disproportionnées au regard des règles de nomination des autres membres de la CNIL.

Mme la garde des Sceaux. Je partage cet avis

Mme Danièle Obono. Quant à notre amendement CL27, il visait, à titre expérimental, à télédiffuser certaines délibérations de la CNIL pour des raisons de transparence mais aussi pour des raisons pédagogiques. Une telle mesure nous paraît de nature à renforcer le sentiment de proximité avec les institutions et les citoyens et les citoyennes verraient comment et par qui et dans quelles conditions des sanctions sont prises. Cela pourra même peut-être encourager la CNIL à ne pas avoir la main qui tremble quand il s'agira de sanctionner les GAFA (Google, Amazon, Facebook, Apple). Nous entendons donc engager l'action de la CNIL dans un cercle vertueux.

Mme la rapporteure. Je suis très sensible à cet argument ; je vous propose que nous tâchions, d'ici à l'examen du texte en séance, de trouver les points qui, dans l'ordre du jour de la CNIL, pourraient être rendus publics.

M. Philippe Gosselin. Madame la rapporteure, je me permets d'appeler respectueusement et amicalement votre attention sur le fait que l'amendement a trait aux délibérations de la commission réunie en formation restreinte, qui est la formation de jugement de la CNIL, celle qui prononce des sanctions et dont les délibérations doivent respecter un certain nombre de conditions de forme. Une telle mesure soulèverait donc d'importantes difficultés au plan non pas matériel mais juridique.

Mme la rapporteure. C'est bien la raison pour laquelle je suis défavorable à la publicité des délibérations, tout en proposant de creuser cette idée pour d'autres travaux de la CNIL.

M. Philippe Latombe. Je complète l'intervention de notre collègue Gosselin : Cet amendement visait la diffusion des délibérations de la CNIL en formation restreinte mais de surcroît en direct, autrement dit sans le moindre filtre susceptible d'assurer la sécurité des délibérations. Le dispositif proposé n'était donc pas acceptable en l'état.

La Commission ***adopte*** *les amendements identiques CL248, CL18 et CL60.*

En conséquence, l'article 2 est ***ainsi rédigé*** *et les trois amendements identiques CL66 de M. Philippe Gosselin, CL71 de M. Éric Bothorel et CL75 de Mme Constance Le Grip, de même que les amendements CL26 de Mme Danièle Obono et CL27 de M. Ugo Bernalicis* ***tombent****.*

Article 2 bis (nouveau)

(art. 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Délégation de certaines missions au secrétaire général de la CNIL

Résumé du dispositif et effets principaux :

Cet article a pour objet de permettre à la CNIL de déléguer au secrétaire général l'exercice de sa mission consistant à informer les auteurs de plaintes ou de réclamations des suites données à celles-ci. Il doit ainsi permettre à cette autorité de mieux traiter les nombreuses réclamations individuelles qu'elle reçoit chaque année.

*

* *

La Commission examine l'amendement CL249 de la rapporteure.

Mme la rapporteure. Il s'agit d'autoriser la CNIL à déléguer à son secrétaire général la charge d'informer les auteurs des réclamations, des pétitions et des plaintes des suites qui sont données à celles-ci, afin de simplifier le traitement de ces réclamations.

La Commission ***adopte*** *l'amendement. L'article 2* bis *est ainsi rédigé.*

Article 3

(art. 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Conditions de délibération de la formation restreinte de la CNIL

Résumé du dispositif et effets principaux :

Le présent article propose de préciser les conditions de délibération de la formation restreinte de la CNIL chargée de prononcer d'éventuelles sanctions à l'encontre des responsables de traitement.

Dernières modifications législatives intervenues :

L'article 6 de la loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits prévoit que seule la formation restreinte peut prononcer des sanctions.

Modifications adoptées par la commission des Lois :

La Commission a approuvé l'économie générale de cet article, sous réserve de modifications rédactionnelles ou de coordination.

Les dispositions de cet article ont été intégrées dans le présent projet de loi à la suite de l'avis du Conseil d'État [(1)] qui soulignait que par « *souci de rehausser au niveau de la loi les garanties d'impartialité exigées par la jurisprudence constitutionnelle à propos du pouvoir de sanction des autorités administratives indépendantes* », il convenait d'apporter deux modifications aux conditions de tenue des séances de la formation restreinte.

1. Les modalités de formation et de réunion de la CNIL

La CNIL se réunit en principe en formation plénière [(2)]. Toutes ses délibérations sont alors prises sur le fondement d'un projet de délibération et, le cas échéant, d'un rapport.

De manière à garantir une séparation stricte entre les fonctions de poursuite, d'instruction et de sanction, l'article 17 de la loi du 6 janvier 1978 [(3)] prévoit toutefois que ces dernières ne peuvent être prononcées à l'encontre des responsables de traitements qui ne respectent pas leurs obligations **qu'en formation restreinte**, réunie sur convocation du président de la CNIL.

Dans ce cas, les membres de cette formation ne peuvent pas participer à l'exercice des attributions de la CNIL en matière :

— de réclamation ou plainte ;

— de dénonciation d'infraction au ministère public ;

— de contrôle.

---

(1) Avis n° 393836 du 7 décembre 2017 sur un projet de loi d'adaptation du droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) L'article 15 de la loi du 6 janvier 1978 prévoit ainsi que « sous réserve des compétences du bureau et de la formation restreinte, la commission se réunit en formation plénière *».*

(3) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Par ailleurs, selon l'article 18 de cette même loi, le commissaire du Gouvernement peut assister à toutes les délibérations de la commission, qu'elle soit réunie en formation plénière ou en formation restreinte. Toutefois, un décret du 20 octobre 2005 revient sur cette possibilité pour les délibérations en formation restreinte de manière à mieux garantir l'indépendance de cette dernière [(1)].

Le commissaire peut également, sauf en matière de sanctions, provoquer une seconde délibération, qui doit intervenir dans les dix jours de la délibération initiale.

Le décret de 2005 précise enfin que si un agent des services de la commission, faisant office de secrétaire de séance, peut être désigné par le président de la formation restreinte, il assiste au délibéré en cette seule qualité et sans y prendre part.

2. Le droit proposé

Le présent article propose d'inscrire ces deux limitations actuellement prévues par décret dans la loi du 6 janvier 1978 précitée. Il permet en cela de consolider les garanties d'indépendance dont bénéficie la CNIL.

Au-delà de mesures de coordination, **l'alinéa 3** introduit à l'article 17 précité l'interdiction pour les agents de la commission d'assister au délibéré de la formation restreinte, à l'exception de ceux chargés du secrétariat.

L'article 18 est également modifié de manière à prévoir que le commissaire du Gouvernement :

— assiste à toutes les délibérations de la commission réunie en formation plénière ainsi que de son bureau lorsque celui-ci se voit chargé d'exercer certaines de ses attributions ;

— peut assister aux réunions de la formation restreinte, sans être présent au délibéré. Il est alors rendu destinataire de l'ensemble des avis et décision de la commission et de la formation restreinte (**alinéa 5**).

L'alinéa 7 introduit une coordination au même article concernant la seconde délibération pouvant être provoquée par le commissaire du Gouvernement qui n'appelle pas de commentaires particuliers.

*

* *

(1) L'article 77 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que « la formation restreinte statue hors la présence du rapporteur et du commissaire du Gouvernement. *»*

*La Commission **adopte** l'amendement de précision CL97 de la rapporteure.*

*Puis elle **adopte** l'article 3 **modifié**.*

Article 4

(art. 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Moyens de contrôle des agents de la CNIL

Résumé du dispositif et effets principaux :

Le présent article précise la rédaction des moyens de contrôle dont disposent les agents de la CNIL et prévoit :

– les conditions limitatives dans lesquelles le secret peut leur être opposé, notamment le secret médical ;

– la possibilité de recourir à une identité d'emprunt dans le cadre du contrôle des services de communication au public en ligne.

Dispositions du règlement : articles 55, 57, 58 et 90 du règlement.

Dernières modifications législatives intervenues :

– la loi du 6 août 2004 (1) a renforcé les pouvoirs de contrôle sur pièce et sur place de la CNIL ;

– la loi du 29 mars 2011 (2) a prévu une information effective du responsable de locaux professionnels sur son droit à s'opposer à la visite des agents de la CNIL ;

– la loi du 17 mars 2014 (3) a permis à la CNIL de procéder à des contrôles en ligne.

Modifications adoptées par la commission des Lois :

La Commission a approuvé l'économie générale de cet article, sous réserve de modifications rédactionnelles ou de coordination.

1. L'état du droit

Dans le cadre de la transposition de la directive du 24 octobre 1995 par la loi du 6 août 2004 précitée, les pouvoirs de contrôle de la CNIL ont été significativement renforcés (4).

(1) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits.

(3) Loi n° 2014-344 du 17 mars 2014 relative à la consommation.

(4) Cette directive prévoit que chaque autorité de contrôle au niveau national doit disposer de pouvoirs effectifs d'intervention lui permettant « d'ordonner le verrouillage, l'effacement ou la destruction de données ou interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement *» et de pouvoirs d'investigation, «* tels que le pouvoir

L'article 44 de la loi du 6 janvier 1978 [1] prévoit ainsi les modalités de ces contrôles, selon qu'ils sont réalisés **sur place, sur pièce, sur audition ou en ligne** pour vérifier le respect des obligations qui incombent aux responsables de traitement.

Ils complètent le contrôle *a priori* que réalise la CNIL dans le cadre des formalités préalables conditionnant l'autorisation des traitements.

a. Des prérogatives de contrôle étendues et encadrées par le juge

Les I et II de l'article 44 dressent le cadre d'intervention de la CNIL pour les contrôles sur place.

Ses membres ainsi que les agents de ses services qui ont été habilités ont accès, de 6 heures à 21 heures [2], à tout lieu à usage professionnel dans lequel sont réalisés des traitements de données personnelles, à l'exclusion des parties affectées, le cas échéant, au domicile privé [3].

L'intervention de la CNIL est toutefois encadrée. Le procureur de la République territorialement compétent doit être informé au moins 24 heures avant le contrôle, ainsi que le responsable des locaux [4] au plus tard lors de l'arrivée des agents sur place. Ce dernier peut alors faire usage d'**un droit d'opposition à la visite**.

Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter.

Toutefois, afin de permettre à la CNIL de réaliser des contrôles inopinés lorsque **l'urgence, la gravité des faits** à l'origine du contrôle ou **le risque de destruction ou de dissimulation de documents** le justifient, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.

Dans ces deux cas, le juge doit statuer dans un délai de 48 heures et la visite s'effectue sous son autorité et son contrôle, en présence de l'occupant des lieux ou de son représentant qui **peuvent se faire assister d'un conseil de leur choix [5]**.

---

d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. »

(1) Dont les dispositions sont complétées par celles du décret modifié n° 2005-1309 du 20 octobre 2005.

(2) Ces horaires s'appliquent également aux perquisitions judiciaires ainsi qu'aux contrôles effectués par l'Autorité des marchés financiers (AMF).

(3) Cette exclusion est conforme à la jurisprudence constante du Conseil constitutionnel qui protège les lieux d'habitation exclusivement privatifs.

(4) Ce dernier peut ne pas être le responsable du traitement, par exemple lors d'un contrôle se déroulant dans les locaux d'un prestataire.

(5) À défaut, ce contrôle peut également se dérouler en présence de deux témoins.

Par ailleurs, conformément au III de l'article 44 précité, les membres de la commission et ses agents habilités peuvent :

— demander **communication de tous documents** nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie [(1)]. Ils peuvent ainsi accéder aux programmes informatiques et aux données, et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle ;

— recueillir, sur place ou **sur convocation**, tout renseignement et toute justification utiles ;

— être assistés par des experts à la demande du président de la CNIL ;

— procéder à toute constatation utile. Ils peuvent, à ce titre, à partir d'un service de communication au public **en ligne**, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant, en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations.

Il est, par ailleurs, précisé à l'article 21 de la loi du 6 janvier 1978 que « *sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions.* »

b. Les règles spécifiques encadrant la communication de données médicales

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

Ce médecin est désigné, à la demande de la CNIL, par le préfet ou, le cas échéant, par l'Agence régionale de santé compétente. Il peut également être désigné par le président de la CNIL s'il est inscrit sur une liste d'experts judiciaires.

c. Les règles spécifiques encadrant la communication de certains traitements réalisés par l'État

Les traitements intéressant la sûreté de l'État et qui sont dispensés de la publication de l'acte réglementaire qui les autorise ne sont pas soumis aux contrôles de la CNIL.

---

(1) La notion de document s'entend alors de façon large et peut comprendre des codes-sources par exemple.

Les contrôles réalisés par la CNIL en 2016

Selon son rapport d'activité pour l'année 2016, la CNIL a réalisé 460 contrôles, dont 100 contrôles en ligne et 94 contrôles portant sur les systèmes de vidéo protection, plus de 30 contrôles sur place et 5 auditions dans ses locaux.

70 % des contrôles réalisés ont porté sur le secteur privé (dont 90 % des contrôles en ligne) et 30 % sur le secteur public.

Cette activité de contrôle devrait continuer à s'accentuer en application du nouveau cadre de protection des données de santé défini par le règlement européen et reposant sur des acteurs davantage responsabilisés en contrepartie de contrôles et de sanctions renforcés.

2. Le dispositif proposé

a. Les dispositions du règlement européen

Les articles 57 et 58 du règlement définissent réciproquement les missions de contrôle et les pouvoirs pour les exercer confiés aux autorités de contrôle.

Par ailleurs, ce dernier article prévoit que « *chaque État membre peut prévoir, par la loi, que son autorité de contrôle dispose de pouvoirs additionnels* » à ceux qu'il mentionne.

L'article 90 prévoit une seconde marge de manœuvre pour les États membres en matière de secret professionnel. Ces derniers peuvent ainsi « *adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle à l'égard des responsables du traitement ou des sous-traitants qui sont soumis à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes, lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret.* »

L'article 55 du règlement prévoit enfin que les autorités de contrôle ne sont pas compétentes « *pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle* ».

b. Une extension des lieux pouvant être contrôlés

L'alinéa 2 supprime la précision selon laquelle les locaux pouvant faire l'objet d'un contrôle sur place sont ceux à usage professionnel de manière à inclure dans ce contrôle les parties communes dans lesquelles peuvent se trouver, par exemple, des éléments de stockage de certaines données. Cette disposition ne remet pas en cause la protection du domicile privé.

c. Les conditions d'accès ou de communication de certaines données

Les alinéas 6 et 7 précisent que :

— l'accès aux programmes informatiques et aux données doit s'effectuer **dans des conditions préservant la confidentialité à l'égard des tiers** ;

— le secret ne peut être opposé aux agents de la CNIL sauf concernant les informations couvertes par **le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou par le secret médical** ;

— pour ce dernier, la communication de données médicales relevant de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé pourra être requise, non plus obligatoirement par un médecin, comme le prévoit le droit en vigueur, mais sous son autorité et en sa présence.

L'alinéa 9 prévoit, quant à lui, la possibilité pour les agents de la CNIL de faire usage d'une identité d'emprunt, notamment dans le cadre de leurs contrôles en ligne afin de renforcer leur efficacité [(1)].

Le recours à une telle identité serait sans incidence sur la régularité des constatations effectuées.

Enfin, conformément à l'article 55 du règlement précité, **l'alinéa 11** prévoit que la CNIL n'est pas compétente pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle. Les principes de séparation des pouvoirs et d'indépendance de l'autorité judiciaire sont ainsi respectés.

*

* *

*La Commission **adopte** successivement l'amendement de coordination CL250 et l'amendement rédactionnel CL98, tous deux de la rapporteure.*

Puis elle examine les amendements identiques CL64 de M. Philippe Gosselin et CL76 de Mme Constance Le Grip.

M. Philippe Gosselin. L'amendement CL64 est défendu.

Mme Constance Le Grip. Cet amendement vise à assurer la cohérence du texte avec l'article 58-1-e) du Règlement général sur la protection des données, qui précise que les autorités de contrôle peuvent obtenir l'accès à « *tous les*

(1) Pour mémoire, les agents de l'AMF peuvent d'ores et déjà recourir à des identités d'emprunt dans le cadre de leurs contrôles.

documents nécessaires à l'accomplissement de leur mission ». Cette mention figure, du reste, à l'article 44 de la loi « Informatique et libertés » de 1978.

Mme la rapporteure. Cette précision est bienvenue. Avis favorable.

La Commission ***adopte*** *ces amendements.*

Elle est ensuite saisie de l'amendement CL28 de Mme Danièle Obono.

Mme Danièle Obono. Cet amendement technique vise à supprimer une incertitude juridique relevée par la CNIL dans l'un de ses avis, en ajoutant l'adverbe « notamment », qui permet plus de flexibilité.

Mme la rapporteure. Le Gouvernement a tenu compte de l'avis que la CNIL a émis sur l'avant-projet de loi : il a lui-même ajouté l'adverbe « notamment ». Votre amendement étant ainsi satisfait, je vous suggère de le retirer.

L'amendement est ***retiré****.*

La Commission examine ensuite l'amendement CL77 de Mme Constance Le Grip.

Mme Constance Le Grip. Cet amendement tend à supprimer la dernière phrase de l'alinéa 6 de l'article 4, qui dispose que le secret professionnel n'est pas opposable aux agents de l'autorité de contrôle. Il s'agit d'éviter toute surtransposition et de rester le plus fidèle possible au texte du RGPD.

Mme la rapporteure. Avis défavorable.

Mme la garde des Sceaux. Avis défavorable. Votre amendement aurait pour effet de supprimer l'obligation de lever le secret lors des contrôles réalisés par la CNIL. En la matière, les négociations avec les autres États membres n'ont pas permis d'aboutir à une harmonisation des dispositions. C'est la raison pour laquelle l'article 90 du règlement offre aux États une marge de manœuvre pour adopter des règles spécifiques en matière de secret. Le Gouvernement a souhaité utiliser cette marge de manœuvre pour renforcer l'exercice de ses missions par la CNIL en prévoyant une levée du secret, sauf lorsqu'il s'agit – et ces trois cas sont traditionnels en droit français – du secret entre l'avocat et son client, du secret des sources journalistiques et, sous certaines conditions, du secret médical.

La Commission ***rejette*** *l'amendement.*

Elle examine ensuite les amendements CL58 de M. Rémy Rebeyrotte, CL63 de M. Philippe Gosselin, CL72 de M. Éric Bothorel et CL78 de Mme Constance Le Grip.

M. Rémy Rebeyrotte. L'amendement CL58 est défendu et, puisque M. Bothorel l'a inspiré, je lui laisse bien volontiers la parole.

M. Éric Bothorel. L'amendement CL72, en quelque sorte rédactionnel, vise à souligner l'importance du respect du secret médical.

M. Philippe Gosselin. Ces amendements ne sont pas purement rédactionnels. On a souligné un peu plus tôt la nécessité de partager les données personnelles de santé. Il s'agit de donner un peu plus de poids au secret médical, moyennant une meilleure prise en compte de ces données.

Mme Constance Le Grip. L'amendement CL78 est défendu.

Mme la rapporteure. Je suis favorable à cet amendement.

Mme la garde des Sceaux. Cette précision me paraît bienvenue. Avis favorable.

La Commission ***adopte*** *ces amendements.*

Elle est ensuite saisie des amendements identiques CL62 de M. Philippe Gosselin et CL79 de Mme Constance Le Grip.

M. Philippe Gosselin. Dans le prolongement des amendements précédents, nous proposons que la communication des données médicales individuelles ne puisse se faire qu'après une information préalable du patient.

Mme la rapporteure. Vous proposez que le patient soit informé lorsque le secret médical est levé dans le cadre de contrôles de la CNIL, mais on considère que celle-ci agit en faveur des patients. En outre, une telle disposition pourrait entraver ou compliquer ces contrôles, notamment si les patients concernés sont nombreux. De ce fait, j'émets un avis défavorable.

La Commission ***rejette*** *ces amendements.*

Puis elle examine les amendements identiques CL61 de M. Philippe Gosselin et CL80 de Mme Constance Le Grip.

M. Philippe Gosselin. Il s'agit de permettre à la CNIL d'effectuer sous une identité d'emprunt des contrôles en ligne des services de communication au public.

Mme Constance Le Grip. La CNIL a déjà la possibilité, depuis 2014, d'effectuer des contrôles sous une identité d'emprunt. Mais nous proposons de préciser explicitement que cette possibilité est exclusivement réservée aux contrôles « en ligne », au risque effectivement d'alourdir la phrase.

Mme la rapporteure. J'approuve l'esprit de ces amendements. Je suggère toutefois que les mots : « en ligne » soient insérés après le mot : « opération » plutôt qu'après le mot : « contrôle ». Si leurs auteurs approuvent cette rectification, j'émettrai un avis favorable à ces amendements.

M. Philippe Gosselin et Mme Constance Le Grip. D'accord.

La Commission ***adopte*** *les amendements CL61 et CL80* ***tels qu'ils viennent d'être rectifiés****.*

Elle ***adopte*** *ensuite l'amendement de précision CL100 de la rapporteure.*

Puis elle ***adopte*** *l'article 4* ***modifié****.*

Article 5

(art. 49 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Coopération entre les autorités de contrôle européennes

Résumé du dispositif et effets principaux :

Le présent article prévoit que :

– conformément aux dispositions du règlement (UE) 2016/679, la CNIL met en œuvre des procédures de coopération et d'assistance mutuelle avec les autres autorités de contrôle européennes concernées ;

– le président de la CNIL est compétent pour inviter d'autres autorités de contrôle à participer à des opérations conjointes de contrôle ;

– ce dernier peut habiliter, à ce titre, les agents de l'autorité de contrôle étrangère, présentant des garanties comparables à ceux de la CNIL, pour exercer tout ou partie des pouvoirs de vérification et d'enquête ;

– les conditions du respect du contradictoire sont précisées ainsi que les conditions de saisine du Comité européen à la protection des données (CEPD).

Dispositions du règlement : chapitre VII du règlement.

Dernières modifications législatives intervenues :

La loi du 6 août 2004 [(1)] a introduit des dispositions de coopération souple entre les autorités de contrôle des différents États membres.

Modifications adoptées par la commission des Lois :

La Commission a approuvé l'économie générale de cet article, sous réserve de modifications rédactionnelles ou de coordination.

(1) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

I. L'ÉTAT DU DROIT

La première étape d'une coopération européenne en matière de protection des données personnelles a été adoptée dans la loi du 6 août 2004, conformément à l'article 28 de la directive du 24 octobre 1995 selon lequel « *chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre* ».

Selon l'article 49 de la loi du 6 janvier 1978, la CNIL peut ainsi, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre État membre, procéder à des vérifications et ordonner des sanctions dans les mêmes conditions et selon les mêmes procédures que celles prévues au niveau national.

La commission est également habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autres autorités de contrôle européennes.

Ces dispositions ne s'appliquent cependant pas aux traitements de souveraineté, à savoir ceux concernant la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, ainsi que l'exécution des condamnations pénales et des mesures de sûreté.

La CNIL est également un membre actif du « groupe de l'article 29 », instauré par cette même directive, qui regroupe les représentants de chacune des autorités de contrôle des États membres. Ce dernier a pour mission d'examiner toute question portant sur la protection des données personnelles, de contribuer à leur mise en œuvre homogène, d'établir un rapport annuel sur l'état de protection de ces données dans l'Union européenne et dans les pays tiers, d'émettre des avis, d'apporter des conseils, etc.

Par ailleurs, l'article 49 *bis* prévoit, quant à lui, des dispositions analogues pour les autorités de contrôle situées dans un État non membre de l'Union européenne « *dès lors que celui-ci offre un niveau de protection adéquat des données à caractère personnel* ».

II. LE DISPOSITIF PROPOSÉ

1. Les dispositions du règlement européen

Le règlement européen a entendu promouvoir la protection la plus homogène et efficace possible des données personnelles sur l'ensemble du territoire de l'Union européenne.

À cette fin, il comporte des dispositions précises au sein du chapitre VII sur la mise en œuvre d'un mécanisme de coopération territoriale et de cohérence entre les différentes autorités compétentes :

— l'article 60 prévoit les modalités de coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées par un traitement ;

— l'article 61 définit les contours de l'assistance mutuelle que devront s'apporter les autorités européennes ;

— l'article 62 décrit les conditions de réalisation des opérations conjointes entre plusieurs autorités de contrôle ;

— l'article 63 traite du mécanisme de cohérence reposant sur les avis du CEPD (article 64) et sur des procédures de règlement d'éventuels litiges (article 65) ;

– l'article 66 prévoit des procédures d'urgence pouvant être mises en œuvre.

Les autres dispositions de ce chapitre définissent les modalités des échanges d'information entre autorités (article 68), ainsi que le rôle et la composition du CEPD (articles 69 à 76).

Ces dispositions témoignent du souhait de construire un véritable droit de la protection des données personnelles en Europe, à la hauteur des enjeux posés par le développement des technologies numériques et en capacité d'accompagner les acteurs de ce secteur ou tous les responsables amenés à traiter des données personnelles dans un cadre juridique sécurisé, assurant la promotion de bonnes pratiques.

2. Les dispositions proposées

Le présent article prévoit la mise en œuvre d'un système de coopération reposant sur une autorisation d'intervention des autres autorités par l'autorité nationale et le contrôle par cette dernière des agents habilités par les autres États membres.

Le droit national s'impose pour les traitements réalisés lors d'opérations conjointes, dans un souci partagé par les États membres d'assurer le respect de la souveraineté nationale.

Par ailleurs, de manière à assurer la coopération de toutes les autorités de contrôle, la seule marge de manœuvre laissée aux États membres concerne les pouvoirs d'enquête confiés aux membres et agents associés aux opérations conjointes.

L'article 49, dans la rédaction proposée, renvoie désormais aux conditions prévues aux articles 60 à 67 du règlement pour la mise en œuvre par la CNIL des procédures de coopération et d'assistance mutuelle avec les autorités de contrôle des autres États membres de l'Union européenne, ainsi que pour la réalisation d'opérations conjointes (**alinéa 2**).

Plusieurs dispositions sont, par conséquent, introduites dans le droit national pour tirer les conséquences de ce nouveau cadre de coopération européen.

Un nouvel article 49-1 prévoit ainsi que :

— la CNIL, qu'elle agisse en tant qu'autorité de contrôle chef de file ou en tant qu'autorité concernée [(1)], est compétente pour traiter une réclamation ou une éventuelle violation des dispositions du règlement affectant par ailleurs d'autres États membres. Le président de la commission invite alors les autres autorités de contrôle concernées à participer aux opérations conjointes qu'il décide de conduire (**alinéa 6**) ;

— les membres et agents de ces autorités peuvent participer à ces opérations lorsqu'elles se déroulent sur le territoire national et être habilités, par le président de la CNIL, s'ils présentent des garanties comparables à celles requises des agents de la commission, à exercer, sous son autorité, tout ou partie des pouvoirs de vérification et d'enquête dont disposent ces derniers (**alinéa 7**) ;

— le président de la CNIL se prononce également sur le principe et les conditions de la participation à une opération conjointe proposée par une autre autorité sur son propre territoire et désigne, le cas échéant, les membres et agents habilités pour y participer (**alinéa 8**).

Un nouvel article 49-2 prévoit, quant à lui, les mesures relatives à la coopération entre autorités de contrôle pour les données personnelles relevant de la directive (UE) 2016/680 (**alinéa 9**). Dans ce cadre :

— la CNIL communique aux autorités de contrôle des autres États membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que des mesures de consultation, d'inspections et d'enquête (**alinéa 10**) ;

— elle répond également aux demandes d'assistance mutuelle formulées par une autre autorité dans un délai ne pouvant excéder un mois et ne peut se soustraire à cette obligation que si elle n'est pas compétente ou si une disposition

---

(1) Selon l'article 4 du règlement, l'« autorité de contrôle concernée» est « une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

« a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève;

« b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être; ou

« c) une réclamation a été introduite auprès de cette autorité de contrôle *»*.

du droit de l'Union européenne ou du droit français y fait obstacle (**alinéa 11**). En contrepartie, elle bénéficie du même droit de formuler des demandes auprès d'une autre autorité (**alinéa 13**).

Le nouvel article 49-3 concerne plus spécifiquement les obligations de la CNIL en tant qu'autorité de contrôle chef de file s'agissant d'un traitement transfrontalier au sein de l'Union européenne. Dans ce cas :

— elle communique le rapport réalisé sur le traitement, ainsi que l'ensemble des informations utiles de la procédure ayant permis de l'établir aux autres autorités de contrôle concernées sans tarder et avant l'éventuelle audition du responsable du traitement ou du sous-traitant. Ces dernières sont alors mises en mesure d'assister aux auditions par tout moyen de retransmission approprié ou de prendre connaissance d'un procès-verbal (**alinéa 15**) ;

— le projet de décision de la formation restreinte est transmis aux autres autorités concernées. Elle doit alors se prononcer sur les objections émises par ces dernières et saisir, si elle décide de les écarter, le CEPD (**alinéa 16**).

Enfin, le nouvel article 49-4 prévoit que lorsque la CNIL a agi en tant qu'autorité concernée dans une opération conjointe, le président est saisi des projets de mesures correctrices proposées par l'autorité chef de file.

Lorsque ces mesures sont équivalentes à celles qu'il peut prononcer (avertissement sur le risque emporté par le traitement ou mise en demeure), le président peut décider d'émettre une objection (**alinéa 19**).

Dans le cas où ces mesures correspondent à des mesures pouvant être prononcées par la seule formation restreinte, le président saisit cette dernière qui peut également prononcer une objection à laquelle l'autorité chef de file devra répondre (**alinéa 20**).

*
* *

*La Commission **adopte** successivement l'amendement de coordination CL252, l'amendement de précision CL101, l'amendement rédactionnel CL102 et l'amendement de précision CL103, tous de la rapporteure.*

Elle est ensuite saisie de l'amendement CL29 de M. Ugo Bernalicis.

Mme Danièle Obono. Cet amendement vise à renforcer la transparence et la collégialité des décisions importantes prises par la CNIL. Nous proposons que, lorsque celle-ci autorise des agents publics d'autres États membres à participer à des enquêtes conjointes en France, la décision soit prise, non pas par le seul président de l'autorité, mais par son assemblée plénière. Cet amendement s'inscrit dans les marges de transposition laissées par la directive, puisque celle-ci ne précise pas les modalités d'habilitation de ces agents.

Mme la rapporteure. Ce type d'opérations conjointes, auxquelles la CNIL a indiqué vouloir participer autant que possible, impose de réagir très rapidement. Il est donc plus adapté que la décision soit prise par le président de l'autorité. Avis défavorable.

La Commission ***rejette*** *l'amendement.*

Puis elle ***adopte*** *successivement l'amendement de précision CL104, l'amendement rédactionnel CL105, l'amendement de cohérence CL106, l'amendement de précision CL108, les amendements rédactionnels CL109 et CL110, l'amendement de précision CL112, l'amendement rédactionnel CL113 ainsi que les amendements de cohérence CL114 et CL115, tous de la rapporteure.*

Elle est ensuite saisie de l'amendement CL31 de M. Ugo Bernalicis.

Mme Danièle Obono. Charles Pasqua affirmait que la démocratie s'arrêtait là où commence la raison d'État…

M. Philippe Gosselin. Si les députés du groupe de La France insoumise se mettent à citer Charles Pasqua, alors là, je dis chapeau ! (*Sourires.)*

Mme Danièle Obono. Eh oui, cela peut nous arriver, à cette heure tardive !

Nous estimons, quant à nous, que les droits et libertés doivent primer sur la raison d'État. C'est pourquoi nous proposons de supprimer l'alinéa 19 de l'article 5, qui nous paraît créer une exception injustifiée et en tout état de cause illégitime.

Mme la rapporteure. Mme la garde des Sceaux s'est déjà exprimée à ce sujet. Nous procéderons peut-être à des auditions complémentaires pour tenter de mieux comprendre cette question d'ici à la séance publique. J'émets donc pour l'instant un avis défavorable.

Mme la garde des Sceaux. Même avis.

La Commission ***rejette*** *l'amendement.*

Puis elle ***adopte*** *l'amendement de coordination CL253, l'amendement de précision CL117 et l'amendement de clarification rédactionnelle CL118, tous de la rapporteure.*

Elle ***adopte*** *ensuite l'article 5* ***modifié****.*

Article 6

(art. 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Mesures correctrices et sanctions

Résumé du dispositif et effets principaux :

Le présent article adapte la possibilité actuellement reconnue à la CNIL de prononcer des mesures correctrices ou des sanctions à l'encontre de responsables de traitement ne respectant pas leurs obligations prévues par le règlement (UE) 2016/679. Il précise à cette fin :

– la répartition des pouvoirs entre le président de la CNIL et la formation restreinte ;

– la nature des nouvelles sanctions pouvant être prononcées, à l'instar des astreintes ou le retrait de certification ou d'agrément ;

– les mesures pouvant être prises par la formation restreinte en cas de procédure d'urgence ;

– le maintien de la publicité des sanctions ;

– l'augmentation du montant des sanctions pécuniaires pouvant être prononcées.

Dispositions du règlement : articles 58, 83 et 84

Dernières modifications législatives intervenues :

– la loi du 6 août 2004 (1) a renforcé les pouvoirs de sanction de la CNIL ;

– la loi du 29 mars 2011 (2) a prévu que seule la formation restreinte peut prononcer des sanctions ;

– la loi du 7 octobre 2016 (3) a augmenté le montant des sanctions pécuniaires pouvant être prononcées (de 150 000 euros à 3 millions d'euros).

Modifications adoptées par la commission des Lois :

La Commission a adopté plusieurs amendements de précision portant sur les sanctions et les décisions que peut prendre la CNIL en cas de non-respect de ses obligations par le responsable d'un traitement. Elle a ainsi clarifié certaines incohérences rédactionnelles et a proposé de remplacer la possibilité de retirer une décision d'approbation d'une règle d'entreprise contraignante par sa suspension partielle ou totale en fonction de la gravité du manquement.

---

(1) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits.

(3) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

I. L'ÉTAT DU DROIT

1. Un pouvoir de sanction récent

Alors que les pouvoirs de la CNIL ont été longtemps limités à la faculté de délivrer des avertissements aux responsables de traitement ou de les dénoncer au parquet en cas de méconnaissance de leurs obligations, la directive du 24 octobre 1995 (1), en imposant aux États membres de renforcer les pouvoirs de contrôle des autorités nationales, lui a permis de disposer de véritables moyens d'intervention et d'une crédibilité nouvelle face aux acteurs concernés.

Cette évolution a d'ailleurs amené le Conseil d'État à considérer que la CNIL « *eu égard à sa nature, à sa composition et à ses attributions, peut être qualifié*[e] *de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* (CEDH) » et qu'en conséquence, elle est tenue, « *lorsqu'elle se prononce sur des agissements pouvant donner lieu aux sanctions prévues par les dispositions des articles 45 et suivants de la loi du 6 janvier 1978* », de statuer « *dans des conditions respectant le principe d'impartialité.* » (2)

Cette obligation est *a priori* assurée depuis la loi du 29 mars 2011 qui désigne la formation restreinte comme seule compétente pour prononcer des sanctions (3).

L'ensemble des mesures et sanctions pouvant être prononcées sont actuellement prévues au chapitre VII de la loi du 6 janvier 1978.

2. Les différentes sanctions prononçables

En application de l'article 45 de la loi du 6 janvier 1978, lorsque le responsable d'un traitement (4) ne respecte pas ses obligations, le président de la CNIL peut le **mettre en demeure de faire cesser son manquement** (5), dans un délai pouvant être ramené à 24 heures en cas d'extrême urgence.

Cette procédure se veut pédagogique et offre au responsable concerné la possibilité de se mettre en conformité avec ses obligations en lui indiquant les mesures à adopter.

---

(1) Transposée par la loi du 6 août 2004 précitée.

(2) CE, 19 févr. 2008, Sté Profil France.

(3) Se reporter au commentaire de l'article 3 du présent projet de loi.

(4) Il peut s'agir d'une personne morale ou, plus rarement, d'une personne physique. Par ailleurs, en l'état du droit, les personnes agissant comme sous-traitants ne peuvent pas faire l'objet de sanction.

(5) Cette mise en demeure peut, le cas échéant, être rendue publique.

S'il n'en tire pas les conséquences, le président peut saisir la formation restreinte qui dispose alors d'un système de sanction gradué en fonction de la gravité du manquement constaté [(1)].

Ces sanctions peuvent prendre la forme :

— d'un avertissement ;

— d'une sanction pécuniaire à l'exception des cas où le traitement est mis en œuvre par l'État ;

— d'une injonction de cesser le traitement.

Par ailleurs, lorsqu'un traitement entraîne **une violation des droits et libertés** mentionnés à l'article 1er de la loi du 6 janvier 1978 [(2)], la formation restreinte, saisie par le président de la commission, peut, dans le cadre d'une procédure d'urgence définie par décret en Conseil d'État :

— décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois ;

— décider le verrouillage de certaines des données traitées, pour une durée maximale de trois mois ;

— informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est mis en œuvre pour le compte de l'État. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

Par ailleurs, en cas d'atteinte grave et immédiate à ces mêmes droits et libertés, le président de la commission peut demander, **par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à leur sauvegarde**.

Conformément à l'article 46, toutes les sanctions prononcées par la formation restreinte doivent l'être sur la base d'un rapport établi par l'un des membres de la CNIL n'y participant pas, à la suite d'une procédure contradictoire, soumise au respect des exigences de l'article 6 de CEDH relatif au droit à un procès équitable.

Des mesures de publicité sont également possibles, à l'instar d'insertion dans des publications ou dans différents supports.

---

(1) Il peut également saisir directement la formation restreinte dans le cas de manquements n'appelant pas de mesures de correction, par exemple, s'ils sont limités dans le temps.

(2) Selon lequel « l'informatique *[…]* ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. *»*

Ces sanctions peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'État (lequel se prononce alors en premier et dernier ressort).

3. Le montant des sanctions pécuniaires

L'article 47 prévoit que le montant des sanctions pécuniaires pouvant être prononcées est proportionné à la gravité du manquement commis et aux avantages que le responsable de traitement en a tiré.

Pour l'apprécier, la formation restreinte prend en compte : le caractère intentionnel ou de négligence du manquement ; les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées ; le degré de coopération avec la commission afin de remédier au manquement ; les catégories de données personnelles concernées et la manière dont la commission a pris connaissance du manquement.

Le montant maximum de la sanction ne peut excéder 3 millions d'euros [(1)] et, peut s'imputer, le cas échéant, sur l'amende prononcée par le juge pénal sur les mêmes faits ou sur des faits connexes. Le seuil a été relevé dans le cadre de la loi pour une République numérique. Il était auparavant de 150 000 euros, ce qui limitait fortement son caractère dissuasif.

4. L'application extraterritoriale des pouvoirs de sanction de la CNIL

L'article 48 précise que les pouvoirs de contrôle et de sanction de la CNIL prévus aux articles 44 [(2)] et 45 peuvent être exercés à l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre État membre de l'Union européenne [(3)].

Les sanctions prononcées par la CNIL en 2016

Selon son rapport d'activité pour l'année 2016, la présidente de la CNIL a prononcé 82 mises en demeure, dont quatre ont été rendues publiques. S'il ne s'agit pas de sanctions à proprement parler, le recours à cette procédure a permis à la majorité des responsables de traitement de se mettre en conformité avec leurs obligations dans des délais adaptés.

La formation restreinte a, quant à elle, prononcé 13 sanctions, dont 9 avertissements (4 publics) et 4 sanctions pécuniaires et publiques.

(1) Article 5 de la loi pour une République numérique.

(2) Se reporter au commentaire de l'article 4 du présent projet de loi.

(3) Toutefois, la CNIL ne peut pas prononcer un avertissement, ni le verrouillage des données dans le cas où le responsable n'est pas situé sur le territoire national lorsque le manquement constitue une violation des droits et libertés reconnus à l'article 1er.

II. LE DISPOSITIF PROPOSÉ

1. Les dispositions prévues par le règlement

Le changement de paradigme dans le contrôle de la protection des données promu par le règlement européen repose sur le passage d'un contrôle *a priori* reposant sur un système de formalités préalables à remplir par les responsables de traitement à **une logique de responsabilisation des acteurs avec pour contrepartie un accroissement des contrôles réalisés *a posteriori* et un durcissement des sanctions**.

Plusieurs dispositions témoignent de cette évolution :

— l'article 58 adapte les pouvoirs des autorités de contrôle et prévoit les mesures correctrices qu'elles pourront prendre ;

— l'article 66 prévoit les mesures d'urgence pouvant être prises par une autorité de contrôle par dérogation au mécanisme de coopération et de contrôle de cohérence prévu par le règlement [(1)] ;

— l'article 83 fixe les conditions dans lesquelles des amendes administratives peuvent être prononcées qui devront être, « *dans chaque cas, effectives, proportionnées et dissuasives* » ;

— l'article 84 accorde une marge de manœuvre aux États membres qui peuvent déterminer « *le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre.* »

2. Une adaptation des mesures correctrices et des sanctions pouvant être prises par la CNIL

Le présent article a pour objet de permettre à la CNIL de compléter les mesures qu'elle peut d'ores et déjà prendre à l'égard de responsables de traitement qui ne respecteraient pas leurs obligations, conformément aux dispositions prévues par le règlement.

Ces mesures s'appliqueront à tous les traitements contrôlés par la CNIL, dont certains ne sont pas soumis au règlement (soit ceux relevant de la directive et ceux hors du champ d'application du droit de l'Union européenne).

L'article 45, dans la rédaction proposée, prévoit ainsi que le président de la CNIL peut **avertir** un responsable de traitement **ou un sous-traitant** du fait que les opérations envisagées **sont susceptibles de violer** les dispositions du règlement ou de la loi du 6 janvier 1978 (**alinéa 4**).

---

(1) Se reporter au commentaire de l'article 5 du présent projet de loi.

Les responsables ou leurs sous-traitants sont ainsi redevables des mêmes obligations, ce qui devrait permettre de contribuer à la diffusion des bonnes pratiques et de responsabiliser l'ensemble des acteurs de la chaîne des traitements.

Si ces derniers n'en tiennent pas compte, le président peut alors saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes (**alinéa 5**) :

— un **rappel à l'ordre** (en lieu et place de l'actuel avertissement) (**alinéa 6**) ;

— une **injonction de mise en conformité** des traitements ou de **satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits**, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une **astreinte** dont le montant ne peut excéder 100 000 euros par jour (**alinéa 7**);

— à l'exception des traitements de souveraineté, **la limitation temporaire ou définitive du traitement [(1)], son interdiction ou le retrait d'une autorisation** (**alinéa 8**) ;

— **le retrait d'une certification** ou l'injonction, à l'organisme concerné, de refuser ou de retirer la certification accordée (**alinéa 9**) ;

— **la suspension des flux de données** adressées à un destinataire situé dans un pays tiers ou à une organisation internationale (**alinéa 10**) ;

— **le retrait de la décision d'approbation d'une règle d'entreprise contraignante** (**alinéa 11**) [(2)] ;

— à l'exception des cas où le traitement est mis en œuvre par l'État, **une amende administrative** (**alinéa 12**) [(3)].

Le montant de cette amende est compris dans des seuils beaucoup plus élevés que ceux en vigueur :

— cette amende ne peut ainsi excéder **10 millions d'euros** ou, s'agissant d'une entreprise, **2 % du chiffre d'affaires annuel mondial** total de l'exercice précédent, le montant le plus élevé étant retenu ;

— ces montants sont portés à **20 millions d'euros et 4 % du chiffre d'affaires** dans le cas du non-respect d'une injonction émise par une autorité de

---

(1) Selon l'article 4, cette limitation consiste en un « marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur *».*

(2) Cette possibilité, non prévue par le règlement, relève de la marge de manœuvre de la France de prendre des mesures correctrices complémentaires conformément à l'article 84 du règlement.

(3) Les mêmes règles d'imputation de l'amende pénale que celles en vigueur sont maintenues à l'alinéa 13.

contrôle ou dans certains cas particuliers mentionnés au 5 de l'article 83 du règlement.

Ces sanctions doivent toutefois être proportionnées au manquement constaté.

Votre rapporteure souligne qu'au regard du faible nombre de sanctions prononcées chaque année par la CNIL, le recours à ces amendes et leur montant devraient être limités.

3. Le maintien de la possibilité pour le président de la CNIL de prononcer des mises en demeure

Le Gouvernement a décidé de recourir à la marge de manœuvre qui lui est laissée par l'article 84 du règlement pour maintenir la possibilité pour le président de la CNIL de prononcer à l'égard d'un responsable de traitement une mise en demeure, rendue publique le cas échéant, de :

— satisfaire aux demandes présentées par une personne en vue d'exercer ses droits (**alinéa 17**) ;

— mettre en conformité les opérations de traitement (**alinéa 18**) ;

— communiquer à la personne concernée une violation de données à caractère personnel (**alinéa 19**) ;

— rectifier ou effacer des données à caractère personnel, ou de limiter le traitement (**alinéa 20**).

4. Les mesures spécifiques en cas de violation des droits et libertés garanties par la protection des données personnelles

a. Les sanctions pouvant être prononcées

L'article 46, dans la rédaction proposée, a pour objet de traiter des sanctions particulières pouvant être prononcées dans le cas de traitements violant les droits et libertés garanties par l'article 1er de la loi du 6 janvier 1978 et le règlement européen.

Ces dispositions reprennent en grande part celles actuellement en vigueur dans les mêmes circonstances. Elles sont toutefois complétées par les mesures prévues par le règlement ou par le Gouvernement en application de la marge de manœuvre qui lui est accordée.

b. Les procédures d'urgence

Conformément à l'article 66 du règlement, si une autorité de contrôle considère qu'il est urgent d'intervenir pour protéger les droits et libertés des personnes concernées, elle peut, par dérogation au mécanisme de contrôle de la

cohérence des décisions prises par les différentes autorités européennes, adopter immédiatement des mesures provisoires visant à produire des effets juridiques sur son propre territoire et ayant une durée de validité déterminée qui n'excède pas trois mois (**alinéa 35**).

Elle informe alors sans délai les autres autorités de contrôle concernées, le Comité européen de la protection des données (CEPD) et la Commission européenne de la teneur de ces mesures et des raisons de leur adoption.

De même, si elle estime qu'une mesure définitive doit être adoptée d'urgence, elle peut demander un avis d'urgence ou une décision contraignante d'urgence au CEPD, en motivant sa demande (**alinéa 36**).

Enfin, pour les traitements relevant de la directive (UE) 2016/680, lorsqu'une autorité de contrôle compétente n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut également demander au CEPD un avis d'urgence ou une décision contraignante d'urgence (**alinéa 37**).

5. Le maintien de la publicité des sanctions

Au-delà de la reprise par l'article 47, dans la rédaction proposée, des dispositions en vigueur sur les conditions de présentation du rapport sur lequel la formation restreinte se fonde pour apprécier les sanctions à prononcer (**alinéa 40**), cet article prévoit que ces dernières peuvent être rendues publiques (**alinéa 41**).

Cette disposition, qui n'est pas prévue par le règlement, découle à nouveau de l'usage par le Gouvernement de la marge de manœuvre qui lui est laissée par l'article 84.

Le Gouvernement considère, en effet, que cette possibilité « *permet une meilleure harmonisation du droit. Elle permet également la sensibilisation des personnes concernées, des responsables de traitement et sous-traitants* » (1).

6. Le retrait de l'agrément des organismes de certification

Enfin, l'article 48, dans la rédaction proposée, prévoit que lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite **a manqué à ses obligations**, le président de la CNIL peut, le cas échéant après mise en demeure, saisir la formation restreinte. Celle-ci peut alors prononcer le retrait de l'agrément qui leur a été délivré.

À ce titre, le Gouvernement souligne, à raison, que « *dans le cadre de la nouvelle logique de responsabilisation prévue par le règlement, ces opérateurs vont jouer un rôle important pour accompagner les responsables de traitement et*

(1) Étude d'impact du présent article, annexée au projet de loi.

les sous-traitants. » Leur activité doit donc être conforme aux obligations introduites par le nouveau cadre juridique de la protection des données personnelles.

*
* *

*La Commission **adopte** successivement les amendements de cohérence CL119 et CL120 de la rapporteure, l'amendement CL261 du Gouvernement et l'amendement de précision CL121 de la rapporteure.*

Elle est saisie de l'amendement CL82 de Mme Constance Le Grip, qui fait l'objet du sous-amendement CL263 de la rapporteure.

Mme Constance Le Grip. Les règles d'entreprise contraignantes – ou *Binding Corporate Rules* (BCR) – sont un instrument juridique européen qui définit les modalités de protection des données transférées au sein d'une même entreprise ou d'un même groupe. Elles sont élaborées de façon vigilante et en étroite concertation avec la Commission nationale de l'informatique et des libertés (CNIL).

Le retrait de la décision d'approbation par la CNIL d'une BCR est un acte administratif lourd de conséquences pour une entreprise. Je suggère donc de substituer aux mots « le retrait » les mots « la suspension partielle ».

Mme Paula Forteza, rapporteure. J'y suis favorable, sous réserve que soit adopté mon sous-amendement précisant que la suspension peut être partielle ou totale.

Mme Christine Hennion. Les BCR concernent les transferts internationaux de données. Une suspension partielle signifierait qu'au sein d'une même entreprise, certaines filiales ne seraient plus concernées par ces règles, ce qui n'a pas de sens par rapport à la responsabilité de la maison-mère. Il convient de prendre garde à un tel amendement, même sous-amendé.

*La Commission **adopte** successivement le sous-amendement CL263, puis l'amendement CL82 ainsi **sous-amendé**.*

*La Commission **adopte** successivement les amendements de cohérence CL122 et CL123, l'amendement de précision CL124, l'amendement de cohérence CL127, les amendements rédactionnels CL128 et CL129, l'amendement de coordination CL254, l'amendement de cohérence CL130, l'amendement de précision CL131 et l'amendement rédactionnel CL132 de la rapporteure.*

*Elle **adopte** ensuite l'article 6 **modifié**.*

CHAPITRE II
Dispositions relatives à certaines catégories de données

Article 7
(art. 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Traitement des données « sensibles »

Résumé du dispositif et effets principaux :

Le présent article a pour objet d'adapter la législation nationale encadrant le traitement des données sensibles aux règles découlant du règlement et de la directive constituant le « paquet européen » adopté en 2016.

Il prévoit principalement d'élargir le champ de ces données aux données biométriques, génétiques ou relatives à l'orientation sexuelle des personnes.

Dispositions du règlement et de la directive concernées : article 9 du règlement et article 10 de la directive.

Dernières modifications législatives intervenues :

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, transposant la directive européenne 95/46 CE, a fixé le cadre actuel du contrôle des traitements portant sur les données sensibles.

Modifications adoptées par la commission des Lois :

La Commission a complété la liste des exceptions au principe d'interdiction des traitements de données sensibles par l'autorisation de réutiliser des données de cette nature dans le cadre de la mise à disposition, en *open data*, des décisions de justice, telle que prévue par la loi du 7 octobre 2016 pour une République numérique, à la condition que cette réutilisation n'ait ni pour objet ni pour effet de permettre la ré-identification des personnes concernées.

I. L'ÉTAT DU DROIT

1. Le principe d'interdiction du traitement des données sensibles

L'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pose le principe de l'interdiction « *de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* »

Cette interdiction se justifie par la nature même de ces données, qui portent sur l'intimité des personnes, ce qui leur confère une sensibilité particulière au regard des usages qui peuvent en être faits.

Le champ des données actuellement concernées par cette interdiction découle de la directive européenne 95/46 CE [1] et de la convention n° 108 du conseil de l'Europe qui fixe comme principe l'interdiction du traitement des données personnelles sensibles « *susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée* » [2].

Cette interdiction s'applique à tous les types de traitements, qu'ils soient automatisés ou non.

2. Les dérogations autorisées

a. Les dérogations accordées à certains traitements

Des dérogations à ce principe sont prévues dans la mesure où la finalité du traitement l'exige pour certaines catégories de données. Elles bénéficient ainsi :

— aux traitements pour lesquels la personne concernée a donné **son consentement exprès**, sauf en cas de disposition législative contraire ;

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

— aux traitements **mis en œuvre par une association** ou tout autre organisme à but non lucratif pour les seules données correspondant à son objet et ne concernant que ses membres ;

— aux traitements portant sur des données à caractère personnel **rendues publiques par la personne concernée** [3] ;

— aux traitements **nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice** [4] ;

— aux traitements nécessaires **aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la**

---

(1) Transposée par la loi n° 2004-801 du 6 août 2004.

(2) Considérant 33 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

(3) À titre d'exemple, le Conseil d'État a considéré que l'appartenance syndicale des candidats aux élections professionnelles constituait une donnée rendue publique par l'intéressé et, en conséquence, de nature à déroger à l'interdiction de collecter en principe de telles données (CE, 28 mars 2014, n° 361042, SNES).

(4) Notamment pour des cabinets d'avocats qui peuvent traiter de telles données dans l'exercice de leur rôle de conseil à leurs clients. Cette faculté a également été reconnue en 2009 par la CNIL à la CIMADE qui assiste les demandeurs d'asile.

gestion de services de santé [1] et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel ;

— aux traitements statistiques **réalisés par l'Insee** ou l'un des services statistiques ministériels, après autorisation de la CNIL et avis du Conseil national de l'information statistique ;

— aux traitements **nécessaires à la recherche, aux études et évaluations dans le domaine de la santé** [2] selon les modalités spécifiques à ce type de données.

b. Les dérogations en cas d'anonymisation

L'interdiction peut également être levée en cas d'anonymisation, dans de brefs délais, des données sensibles.

Pour cela, le procédé d'anonymisation retenu doit, au préalable, avoir été reconnu conforme par la CNIL, qui pourra, sur ce fondement, autoriser le traitement envisagé.

Le droit en vigueur précise, par ailleurs, que les dispositions encadrant spécifiquement le traitement des données de santé ne sont alors pas applicables [3].

Enfin, l'article 8 prévoit que ne sont pas soumis au principe d'interdiction les traitements **justifiés par l'intérêt public** [4] qui sont :

— autorisés par la CNIL ;

— autorisés par décret en Conseil d'État après avis motivé et publié de cette dernière ;

— compris sur une liste des traitements permettant, le cas échéant, de répondre à une situation d'urgence ou à une alerte sanitaire, et qui font l'objet d'une déclaration préalable auprès de la CNIL.

Ces dérogations sont d'interprétation stricte et ne peuvent en aucun cas avoir pour effet de réduire le niveau de protection des individus. Elles doivent *a minima* respecter les exigences résultant des conditions de licéité applicables aux traitements de données personnelles (existence d'un intérêt légitime pour le

(1) Par exemple, dans le cadre de la mise en place du dossier médical partagé.

(2) L'extension de cette dérogation aux études et évaluations dans le domaine de la santé découle de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

(3) A titre d'exemple, la CNIL a autorisé sur ce fondement des traitements en vue d'études épidémiologiques à partir de données issues des feuilles de soins anonymisées à bref délai.

(4) En pratique, ces traitements sont principalement mis en œuvre par les ministères de la défense ou de l'intérieur.

responsable de traitement, consentement des personnes concernées, traitement découlant d'une obligation légale), soit être plus strictes que ces dernières [(1)].

c. Les autres types de données faisant l'objet de procédures particulières

Pour rappel, d'autres types de données font l'objet de procédures d'autorisation particulières, sans pour autant être comprises dans la définition des données sensibles prévue par l'article 8 précité.

Parmi la dizaine de traitements concernés se trouvent notamment ceux portant sur des données génétiques et des données biométriques.

En ce qui concerne les traitements portant sur données génétiques, une exception au régime d'autorisation préalable est prévue par l'article 25 de la loi de 1978 pour ceux d'entre eux qui sont **mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements.**

Ces derniers peuvent, dans ce cas, seulement faire l'objet d'une déclaration auprès de la CNIL.

II. LE DISPOSITIF PROPOSÉ

L'article 7 du projet de loi modifie la rédaction de l'article 8 de la loi du 6 janvier 1978 précité de manière à assurer sa compatibilité avec **l'article 9 du règlement** et **l'article 10 de la directive**.

En effet, si le droit national est proche du droit européen, des différences sémantiques et de champ des données sensibles justifient des adaptations.

Le 4 de l'article 9 du règlement laisse, par ailleurs, une marge de manœuvre à l'appréciation des États membres pour maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données de la santé.

En conséquence, le présent article propose de maintenir le principe d'interdiction des traitements de données sensibles tout en élargissant leur champ **aux données génétiques et biométriques** aux fins d'identifier une personne physique de manière unique, **ainsi qu'aux données concernant l'orientation sexuelle** d'une personne (**alinéa 3**).

« *Dans un souci de cohérence du droit national, ainsi que de sécurité juridique tant pour les responsables de traitements que pour les personnes concernées* », **cette extension s'appliquera à tous les traitements portant sur**

(1) Selon l'avis n° 06/2014 du 9 avril 2014 du Groupe de l'article 29.

ces données, qu'ils relèvent du droit de l'Union européenne ou du droit national [(1)].

Par ailleurs, outre les dérogations prévues par l'article 9 du règlement à ce principe qui reprennent celles d'ores et déjà prévues par le droit national, le présent article prévoit :

— l'introduction d'une dérogation pour les traitements mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques nécessaires aux contrôles de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés ou aux agents (**alinéa 7**), conformément aux recommandations de la CNIL [(2)] ;

— le maintien de la dérogation prévue pour les traitements mis en œuvre par l'État, notamment en matière de données génétiques et biométriques, qui sont justifiés par l'intérêt public et autorisés par décret en Conseil d'État pris après avis motivé et publié de la commission (**alinéa 12**).

Par ailleurs, deux dispositions de coordination entre le droit national et le paquet européen sont proposées :

— le régime d'autorisation préalable est supprimé pour les traitements à des fins statistiques ou ceux portant sur des données faisant l'objet d'un procédé d'anonymisation dans de brefs délais, conformément à l'économie générale du projet de loi qui fait reposer la protection des données sur une responsabilisation accrue des acteurs et leur contrôle par l'autorité régulatrice plutôt que sur un système de formalités préalables (**alinéas 4 et 9**) ;

— la dérogation au principe d'interdiction du traitement des données de santé doit être justifiée par l'intérêt public et le traitement de ces données doit être conforme aux dispositions du chapitre IX qui traite spécifiquement de ces données (**alinéa 5**).

Si la commission des Lois a approuvé l'économie générale de cet article, sous réserve de modifications rédactionnelles ou de précision, elle a toutefois introduit, à l'initiative du Gouvernement, une nouvelle exception au principe d'interdiction des traitements de données sensibles pour ceux portant sur la réutilisation d'informations figurant dans les jugements et décisions de justice rendues publiques en *open data*, conformément à la loi du 7 octobre 2016 pour une République numérique.

*

* *

(1) Étude d'impact du présent article, annexée au projet de loi.

(2) Délibération n° 217-299 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 6 janvier 1978.

La Commission ***adopte*** *l'amendement de précision CL133 de la rapporteure.*

Puis elle examine l'amendement CL260 du Gouvernement.

Mme Nicole Belloubet, garde des Sceaux, ministre de la justice. Cet amendement a pour objet de compléter l'article 8 de la loi du 6 janvier 1978 afin d'autoriser la réutilisation des données sensibles dans le cadre de la mise à disposition du public à titre gratuit des décisions de justice.

L'open data des décisions de justice, introduit par la loi du 7 octobre 2016 pour une République numérique, ouvre de puissantes perspectives d'évolution dans la façon dont la justice est rendue en permettant d'améliorer la qualité des pratiques juridictionnelles par l'analyse des décisions de justice et de renforcer la connaissance de l'ensemble de la jurisprudence.

L'open data se trouve à la confluence de principes fondamentaux, tels que la publicité et la transparence de la justice, le respect de la vie privée des justiciables et des professionnels de la justice et, surtout, la protection des données à caractère personnel.

Le rapport de la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, présidée par le professeur Cadiet, m'a été remis le 9 janvier. Il recommande une modification de la loi informatique et libertés pour la mise en œuvre de l'open data des décisions de justice.

La recommandation n° 17 du rapport préconise de modifier les dispositions de l'article 9 de la loi du 6 janvier 1978 afin de permettre la réutilisation des données de nature pénale contenues dans les décisions de justice diffusées dans le cadre de l'open data. Il s'agit notamment de permettre à des entreprises du secteur de la technologie juridique, les *Legal tech,* qui proposent des logiciels de services juridiques, de pouvoir traiter des données pénales contenues dans les décisions de justice, à des fins commerciales.

Cette recommandation est traduite dans le projet de loi : la réutilisation de telles données figurant dans les décisions de justice est autorisée à l'article 11. Une garantie supplémentaire a été ajoutée : la réutilisation des données ne peut avoir pour objet ou pour effet la réidentification des personnes concernées.

Le rapport préconise également une modification de l'article 8 de la loi de 1978 afin de prévoir que l'interdiction de traitement de données sensibles ne s'applique pas à la réutilisation des décisions de justice diffusées dans le cadre de l'open data, à condition, également, que ces traitements n'aient ni pour objet ni pour effet la réidentification des personnes concernées. Cette recommandation figure également dans l'avis de la CNIL sur le projet de loi, émis le 30 novembre.

Je précise qu'un décret d'application est en cours de préparation, de manière à préciser les modalités de la mise à disposition des décisions, et

notamment les garanties en matière de prévention du risque de réidentification des personnes.

Mme la rapporteure. L'open data est essentiel dans la perspective de la création de nouveaux biens et de nouveaux services ainsi que la mise en œuvre d'un contrôle citoyen effectif, à la condition, évidemment, que ces données soient anonymisées. Avis favorable.

La Commission ***adopte*** *l'amendement CL260.*

Elle ***adopte*** *successivement les amendements de précision CL255 et CL134 et l'amendement rédactionnel CL135 de la rapporteure.*

Elle ***adopte*** *ensuite l'article 7* ***modifié****.*

TITRE II
MARGES DE MANŒUVRE PERMISES PAR LE RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIF À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉEES À CARACTÈRE PERSONNEL ET À LA LIBRE CIRCULATION DE CES DONNÉES, ET ABROGEANT LA DIRECTIVE 95/46/CE

CHAPITRE I^ER
Champ d'application territorial des dispositions complétant le règlement (UE) 2016/679

Article 8
(art. 5-1 [nouveau] de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Champ d'application de la loi nationale en cas de divergence de législations entre États ayant utilisé une marge de manœuvre laissée par le règlement

Résumé du dispositif et effets principaux :

Le présent article règle les modalités d'application territoriale en cas de divergence des législations nationales dans les domaines où les États peuvent préciser les dispositions du règlement général sur la protection des données ou prévoir des garanties supplémentaires par rapport à ce dernier :

– la loi nationale s'appliquera dès lors que la personne réside en France, y compris lorsque le responsable du traitement n'y est pas établi ;

– toutefois, en présence d'un traitement à des fins journalistiques (secteur audiovisuel, presse…), le droit applicable sera celui dont relève le responsable du traitement lorsqu'il est établi au sein de l'Union européenne.

Dispositions du règlement concernées : considérant 153 et article 85.

Dernières modifications législatives intervenues :

La loi du 6 janvier 1978 ne comportait initialement aucune règle sur son champ d'application territoriale. La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, transposant dans notre droit la directive 95/46/CE du 24 octobre 1995, a clarifié le régime applicable aux traitements et à leurs responsables en prévoyant deux critères alternatifs d'applicabilité de la loi française fondés sur la personne responsable du traitement ou le moyen utilisé.

Modifications adoptées par la commission des Lois :

La Commission a adopté cet article sans modification.

1. L'état du droit

Le champ d'application territoriale de la législation relative à la protection des données à caractère personnel est aujourd'hui défini par l'**article 5 de la loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés.

Cette loi s'applique, en l'état du droit issu de la transposition, en 2004, de la directive 95/46/CE du 24 octobre 1995, aux traitements de données à caractère personnel suivants :

— ceux dont **le responsable est établi sur le territoire français**, cette condition étant satisfaite dès lors que le responsable d'un traitement exerce une activité sur le territoire français dans le cadre d'une installation (critère de territorialité de la personne) ;

— à défaut, ceux dont le responsable recourt à des **moyens de traitement situés sur le territoire français**, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre (critère de territorialité du moyen utilisé).

2. Le dispositif proposé

a. Le règlement général sur la protection des données

Parmi les avancées majeures du règlement général sur la protection des données figure l'**extension du champ d'application territoriale des règles européennes de protection des données à caractère personnel en se fondant sur le critère de résidence de la personne concernée**.

L'**article 3 du règlement** prévoit l'application de ses règles :

— non seulement aux traitements de données personnelles mis en œuvre par les responsables de traitements établis dans l'Union européenne (UE) ;

— mais aussi aux traitements mis en œuvre par des responsables établis hors de l'UE dès lors qu'ils visent des **résidents de l'UE, « *lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes* (...), *qu'un paiement soit exigé ou non* » ou « *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »**.

Le règlement, de nature générale, prévoit cependant de nombreuses marges de manœuvre qui permettent aux États membres de préciser certaines dispositions ou de prévoir des garanties supplémentaires par rapport à celles prévues par le droit européen. Il en va ainsi, par exemple, pour les droits de la personne en cause, les obligations du responsable de traitement ou du sous-traitant, le transfert de données vers l'étranger ou encore les pouvoirs des autorités de contrôle.

b. Le projet de loi

Dans un souci de sécurité juridique, il y a lieu de régler les **modalités d'application territoriale des règles nationales en cas de conflit de normes**. Tel est l'objet du présent article qui insère à cette fin un **nouvel article 5-1** dans la loi n° 78-17 du 6 janvier 1978 précitée**.**

i. Le principe : l'application du droit français lorsque la personne concernée réside en France

En **principe**, les règles nationales s'appliqueront **« *dès lors que la personne concernée réside en France*, *y compris lorsque le responsable de traitement n'est pas établi en France* »**, permettant ainsi une lutte efficace contre le phénomène de *forum shopping*.

À titre d'exemple, tout traitement concernant un mineur de moins de 16 ans vivant en France pour lequel le consentement de ses parents n'aurait pas été recueilli sera justiciable des règles françaises [(1)].

ii. L'exception : l'application du droit dont relève le responsable du traitement pour les traitements relatifs à la liberté d'expression et d'information

Par **dérogation**, lorsque seront concernés des **traitements** de données personnelles réalisés **à des fins journalistiques ou d'expression universitaire, artistique ou littéraire** mettant en cause le droit à la liberté d'expression et d'information, **le droit applicable sera celui dont relève le responsable de traitement lorsqu'il est établi dans l'Union européenne**.

(1) À défaut d'une telle précision, le critère d'application du droit français aurait été, en vertu de l'article 3 du code civil, la nationalité du mineur et non son lieu de résidence.

Cette règle spécifique, justifiée par les exigences liées à la protection de la liberté d'expression et d'information, concernerait principalement les traitements de données personnelles « *dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse* » [(1)].

*

* *

La Commission ***adopte*** *l'article 8* ***sans modification****.*

CHAPITRE II
Dispositions relatives à la simplification des formalités préalables à la mise en œuvre des traitements

Article 9
(art. 22 à 25 et 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Suppression des formalités préalables, sauf pour certains traitements de données personnelles particulièrement sensibles

Résumé du dispositif et effets principaux :

Le présent article tire les conséquences de la nouvelle logique de conformité et de responsabilité posée par règlement général sur la protection des données :

– il supprime le régime de déclaration préalable pour les traitements de données non sensibles au profit de l'obligation d'effectuer une analyse d'impact en cas de traitement à risque et, en cas de risque élevé, de consulter la CNIL ;

– il supprime le régime d'autorisation par la CNIL ou par décret en Conseil d'État ou arrêté pris après avis de celle-ci pour les traitements de données sensibles ou mis en œuvre par ou pour le compte de l'État, d'un établissement public ou d'une personne morale de droit privé gérant un service public ;

– il conserve cependant un régime d'autorisation préalable pour certains traitements d'une sensibilité particulière : ceux mis en œuvre pour le compte de l'État et portant sur des données biométriques ou génétiques et ceux mis en œuvre pour le compte de personnes publiques ou privées traitant des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR).

Dispositions du règlement concernées : articles 9, 10, 24, 35 et 36.

Dernières modifications législatives intervenues :

La logique de formalités préalables à laquelle sont aujourd'hui soumis les traitements de données personnelles résulte de la transposition, par la loi du 6 août

(1) Considérant 153 du règlement (UE) 2016/679 du 27 avril 2016.

2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, de la directive 95/46/CE du 24 octobre 1995 qui différenciait les obligations imposées aux responsables de traitements en fonction de la nature des données concernées et du risque que leur traitement pouvait représenter pour les libertés individuelles.

Les dernières évolutions en la matière sont intervenues avec l'assouplissement des conditions d'utilisation du NIR dans le cadre de travaux de santé et de statistique ou de recherche publiques, par les lois du 26 janvier 2016 de modernisation de notre système de santé et du 7 octobre 2016 pour une République numérique.

Modifications adoptées par la commission des Lois :

La Commission a approuvé l'économie générale de cet article, sous réserve de modifications rédactionnelles et de l'adoption d'un amendement de votre rapporteure tendant à réparer une omission.

1. L'état du droit

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et la directive 95/46/CE du 24 octobre 1995 sont en grande partie fondées sur une logique de formalités préalables, que le règlement général sur la protection des données remplace par une logique de conformité et de responsabilité.

Le chapitre IV de la loi de 1978 définit deux types de formalités préalables à la mise en œuvre des traitements : **la déclaration ou l'autorisation**. Le traitement du numéro d'inscription au répertoire (NIR), donnée personnelle particulièrement sensible, est strictement encadré, même si le régime juridique applicable a récemment évolué pour en faciliter l'utilisation à des fins de recherche.

Dans l'ensemble, la gradation des formalités préalables est fonction de l'objet du traitement, de la sensibilité des données traitées et de la nature du responsable du traitement. Ces formalités préalables se sont traduites, pour la Commission nationale de l'informatique et des libertés (CNIL), par la réception, en 2016, de 102 629 dossiers de formalités et 316 demandes d'autorisation en matière de biométrie et la délivrance de 190 autorisations.

a. Le régime de la déclaration

Le **régime de la déclaration**, favorable à l'initiative des responsables de traitements de données puisque le contrôle n'intervient qu'*a posteriori*, est applicable aux fichiers portant sur des données non sensibles. Ce régime est prévu par les **I, I *bis*, III et V de l'article 22**. Cette déclaration peut prendre la **forme classique** posée par l'**article 23** ou être **simplifiée**, voire **dispensée**, dans les conditions fixées par l'**article 24** « *pour les catégories les plus courantes de*

traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés ».

TRAITEMENTS SOUMIS AU RÉGIME DE LA DÉCLARATION (*)

Traitements de données à caractère personnel	Formalité préalable	Disposition
Traitements de droit commun	Déclaration auprès de la CNIL	I de l'article 22
Traitements ayant pour seul objet la tenue d'un registre exclusivement destiné à l'information du public	Pas de formalité préalable	II de l'article 22
Certains traitements mis en œuvre par une association ou un organisme à but non lucratif à caractère religieux, philosophique, politique ou syndical		
Traitements pour lesquels le responsable a désigné un correspondant à la protection des données, sans transfert des données à un pays non membre de l'UE		
Traitements de données de santé mis en œuvre par les organismes ou services chargés d'une mission de service public en vue de répondre, en situation d'urgence, à une alerte sanitaire	Déclaration auprès de la CNIL	V de l'article 22

(*) Hors traitements de données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques.

b. Le régime de l'autorisation

Le **régime de l'autorisation**, plus contraignant, s'applique logiquement aux traitements portant sur des **données sensibles ou mis en œuvre par l'État ou pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public**.

L'autorisation peut être délivrée **soit par la CNIL** (article 25), **soit par le pouvoir exécutif** (articles 26 et 27).

Exemples de traitements soumis au régime de l'autorisation

1/ Autorisation par la CNIL (article 25)

Le traitement de données génétiques par le CNRS dans le cadre d'une étude de la diversité génétique et linguistique de la population du Cap-Vert, les traitements relatifs à la gestion du contentieux lié au recouvrement des contraventions au code de la route et à l'identification des conducteurs dans le cadre des radars de vitesse, le fichier des personnes à risques pour les besoins du système de location de vélos Vélib' ou les systèmes de reconnaissance du réseau veineux des doigts de la main aux fins de contrôle de l'accès aux locaux sur les lieux de travail.

2/ Autorisation par le pouvoir exécutif

– par **arrêté** pris après avis motivé et publié de la CNIL (I de l'article 26) ou non publié (III du même article), comme pour le traitement relatif au suivi du trafic maritime « TRAFIC 2000 » ou le traitement « numérisation des procédures pénales » ;

– par un **acte réglementaire unique** (IV de l'article 26 et III de l'article 27), ce qui est le cas des dispositifs de lecture automatisée de plaques d'immatriculation ;

– par **décret en Conseil d'État** pris après avis motivé et publié de la CNIL (I de l'article 27), à l'instar du traitement facilitant la gestion des conditions matérielles d'accueil des demandeurs d'asile « DNA », l'application de gestion des dossiers des

ressortissants étrangers sollicitant la délivrance d'un visa ou le traitement relatif aux passeports et aux cartes nationales d'identité « TES » ;

– par **arrêté ou décision de l'organe délibérant** (II de l'article 27), comme dans le cas de la décision du conseil départemental des Alpes-Maritimes pour la mise en œuvre d'un traitement aux fins de contrôle du revenu de solidarité active.

TRAITEMENTS SOUMIS AU RÉGIME DE L'AUTORISATION (*)

Traitements de données à caractère personnel	Formalité préalable	Disposition
Traitements statistiques mis en œuvre par l'INSEE et les services statistiques ministériels	Autorisation par la CNIL	I de l'article 25
Traitements de données qui font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci et qui font l'objet d'un procédé d'anonymisation ou sont justifiés par l'intérêt public		
Traitements portant sur des données génétiques, sauf ceux mis en œuvre par des médecins ou biologistes aux fins de médecine préventive, de diagnostics médicaux ou d'administration de soins ou de traitements		
Traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux mis en œuvre par des auxiliaires de justice aux fins de défense des personnes		
Traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de disposition législative ou réglementaire		
Traitements ayant pour objet l'interconnexion de fichiers relevant de personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ou d'autres personnes et dont les finalités sont différentes		
Traitements de données comportant des appréciations sur les difficultés sociales des personnes		
Traitements mis en œuvre par toute personne autre que l'État comportant des données biométriques nécessaires au contrôle de l'identité des personnes		
Traitements mis en œuvre pour le compte de l'État qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté	Autorisation par arrêté du ou des ministres compétents, après avis motivé et publié de la CNIL (**)	I de l'article 26
Mêmes traitements lorsqu'ils font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci	Autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL (**)	II de l'article 26
Traitements de données mis en œuvre pour le compte de l'État portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes	Autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL	I de l'article 27
Mêmes traitements mais portant sur des données génétiques	Autorisation par la loi ou la CNIL	I de l'article 25

Traitements mis en œuvre pour le compte de l'État portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes : – qui ne comportent aucune donnée faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci ; – qui ne comportent aucune donnée relative aux infractions, condamnations et mesures de sûreté ; – qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ; – et qui sont mis en œuvre par des services ayant pour mission de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés ou d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, ou d'établir des statistiques	Autorisation par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant, après avis motivé et publié de la CNIL	II de l'article 27
Traitements relatifs au recensement de la population		

(*) Hors traitements de données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques.

(**) Un décret en Conseil d'État peut dispenser de publication l'acte d'autorisation : seul le sens de l'avis de la CNIL est alors publié, en même temps que le décret autorisant la dispense de publication de l'acte (III de l'article 26).

c. Le régime spécifique applicable au numéro d'inscription au répertoire

Un **régime spécifique, mixte et plus contraignant que le droit commun**, s'applique à l'utilisation du **numéro d'inscription au répertoire (NIR)** national d'identification des personnes physiques (RNIPP) de l'Institut national de la statistique et des études économiques (INSEE).

Plus communément dénommé numéro de sécurité sociale, le NIR est une donnée très identifiante, considérée donc comme particulièrement sensible, justifiant que son utilisation soit entourée d'importantes garanties. Ce régime a été modifiée à deux reprises en 2016 [(1)], afin de faciliter le recours au NIR dans certains domaines, notamment la recherche scientifique publique, ce qui rend sa lecture quelque peu complexe. Les éléments fondant ce régime sont, à titre principal, l'utilisation du NIR qui est envisagée et la qualité de la personne pour laquelle son traitement est mis en œuvre.

(1) Par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé et la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

TRAITEMENTS DE DONNÉES COMPORTANT LE NIR OU IMPLIQUANT LA CONSULTATION DU RNIPP

Traitements de données à caractère personnel	Formalité préalable	Disposition
Traitements comportant le NIR parmi les données traitées mis en œuvre pour le compte ou par…		
… une personne privée	Autorisation par la CNIL	I de l'article 25
… l'État, une personne morale de droit public ou une personne morale de droit privé mettant en œuvre un service public ou le service statistique public	Autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL	I de l'article 27
Traitements impliquant la consultation du RNIPP mis en œuvre pour le compte ou par…		
… une personne privée	Autorisation par la CNIL	I de l'article 25
… l'État, une personne morale de droit public ou une personne morale de droit privé mettant en œuvre un service public ou le service statistique public	Autorisation par arrêté ou décision de l'organe délibérant, après avis motivé et publié de la CNIL	II de l'article 27
Traitements du NIR à des fins de recherche médicale	Autorisation par la CNIL après avis d'un comité d'expertise	Article 54
Traitements de données de santé utilisant le NIR, mis en œuvre par des organismes ou services chargés d'une mission de service public afin de répondre, en cas d'urgence, à une alerte sanitaire	Déclaration auprès de la CNIL dans un cadre défini par décret en Conseil d'État	V de l'article 22
Traitements du NIR à des fins de veille sanitaire ou de gestion des services sanitaires et médico-sociaux	Autorisation par la loi	Article L. 1111-8-1 du code de la santé publique
Traitements du NIR pour l'offre de téléservices aux usagers de l'administration	Autorisation par arrêté ou décision de l'organe délibérant, après avis motivé et publié de la CNIL	II de l'article 27
Traitements du NIR à des fins de statistique publique par l'INSEE *(droit commun)*	Déclaration auprès de la CNIL avec garanties de cryptage	I *bis* de l'article 22
Traitements du NIR à des fins de statistique publique par l'INSEE *(les données traitées sont des données faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci ou des données relatives aux infractions, condamnations et mesures de sûreté)*	Autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL	I de l'article 27
Traitements du NIR à des fins de recherche scientifique ou historique	Autorisation par la CNIL avec garanties de cryptage	I de l'article 25

2. Le dispositif proposé

a. Le règlement général sur la protection des données

Le règlement 2016/679 du 27 avril 2016 substitue à la logique de formalités préalables celle de **responsabilisation des acteurs** tout au long de la mise en œuvre du traitement. L'**article 24** du règlement prévoit ainsi que, « *compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques dont le degré de probabilité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures*

techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ».

Parmi ces mesures figurent la mise en œuvre d'outils de protection des données personnelles dès la conception du traitement ou par défaut (article 25), la désignation d'un délégué à la protection des données par un nombre plus important de responsables (article 37), l'obligation de tenir une documentation, en particulier au travers d'un registre des activités de traitement (article 30), la participation à des mécanismes de certification (articles 42 et 43), l'adhésion à des codes de bonne conduite (articles 40 et 41) ou encore la notification des violations de données personnelles à l'autorité de protection et, dans certains cas, à la personne concernée (articles 33 et 34).

En contrepartie, le pouvoir des autorités de contrôle est renforcé, notamment les sanctions pécuniaires qu'elles sont habilitées à prononcer [(1)].

Cette nouvelle logique conduit à **une réduction importante des formalités préalables**, en particulier la suppression de la plupart des obligations de déclaration préalable dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes concernées. Le système déclaratif était en effet considéré comme une obligation particulièrement lourde pour les acteurs du numérique et d'un intérêt relatif, puisqu'il conduisait à la transmission d'un grand nombre d'informations, d'intérêt inégal, à la CNIL.

Le règlement conserve toutefois des formalités pour les traitements présentant un « *risque élevé pour les droits et libertés des personnes physiques* », en raison, notamment, d'un recours à de nouvelles technologies et « *compte tenu de la nature, de la portée, du contexte et des finalités du traitement* » (**article 35**). Cette analyse d'impact est en particulier obligatoire :

— lorsque le traitement consiste en une « *évaluation systématique et approfondie d'aspects personnels (…), qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques* » ;

— lorsque sont traitées « *à grande échelle* » des données sensibles, qui révèlent l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques, l'appartenance syndicale, des données génétiques, biométriques ou concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives aux condamnations pénales et aux infractions ;

— lorsque le traitement procède à « *la surveillance systématique à grande échelle d'une zone accessible au public* ».

(1) Voir supra*, le commentaire de l'article 6.*

Le contenu de l'analyse d'impact relative à la protection des données

– une description systématique des opérations de traitement et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable ;

– une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard de ses finalités ;

– une évaluation des risques pour les droits et libertés des personnes concernées ;

– les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données et à apporter la preuve du respect du règlement.

Lorsque l'analyse d'impact conclut que « *le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* », la **consultation préalable de l'autorité de contrôle** est obligatoire (**article 36**). Cette autorité pourra interdire le traitement si celui-ci constitue une violation du règlement, « *en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque* ».

Le G29, instance regroupant l'ensemble des autorités de protection des données personnelles de l'Union européenne, a publié des lignes directrices définissant plus précisément les circonstances dans lesquelles l'analyse d'impact sera obligatoire et les conditions de sa mise en œuvre [(1)]. La CNIL a également mis à disposition des entreprises et administrations un logiciel libre destiné à faciliter la conduite et la formalisation d'analyses d'impact telles que prévues par le règlement [(2)].

Le règlement autorise les États à maintenir des régimes plus stricts pour certains types de traitements, en raison de la sensibilité particulière des données traitées, en prévoyant :

— des « ***conditions supplémentaires****, y compris des limitations, en ce qui concerne le traitement des* ***données génétiques, (…) biométriques ou concernant la santé*** » (article 9, § 4) ;

— des **« *garanties appropriées* »** pour le traitement des **données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté** connexes (article 10) ;

— une « ***autorisation préalable*** *en ce qui concerne le traitement effectué par un responsable du* ***traitement dans le cadre d'une mission d'intérêt public*** *exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique* » (article 36, § 5) ;

---

(1) Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « *susceptible d'engendrer un risque élevé* » aux fins du règlement (UE) 2016/679*, adoptées le 4 avril 2017 et modifiées le 4 octobre 2017.*

(2) https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

— des « ***conditions spécifiques*** **[pour le]** ***traitement d'un numéro d'identification national*** *ou de tout autre identifiant d'application générale* » (article 87) ;

— « *des* ***règles plus spécifiques*** » pour les traitements dans le cadre des **relations de travail** (article 88).

Le règlement européen est toutefois sans conséquence sur le régime d'autorisation applicable aux traitements mis en œuvre pour le compte de l'État qui intéressent la sûreté de celui-ci, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté (qui relèvent de l'article 26 de la loi actuelle).

b. Le projet de loi

Le présent article, en cohérence avec les dispositions du règlement général sur la protection des données, procède à trois modifications d'envergure au sein du chapitre IV de la loi n° 78-17 du 6 janvier 1978 précitée.

i. Le remplacement du régime de déclaration préalable par l'obligation de mener une analyse d'impact, voire de consulter l'autorité de protection

La rédaction nouvelle de l'actuel article 22 de la loi de 1978, relatif aux déclarations préalables, proposée par le **I du présent article**, combinée à l'abrogation, par son **III**, de l'article 24 de la même loi, relatif à la simplification et à la dispense des formalités de déclaration pour les traitements de données les moins attentatoires à la vie privée ou aux libertés, conduisent à la **suppression du régime de déclaration préalable** sur lequel notre droit de la protection des données personnelles est fondé depuis 1978.

Ces modifications permettent l'application directe des dispositions du règlement général sur la protection des données relatives à l'obligation de conduire une analyse de l'impact des opérations de traitement sur la protection des données personnelles lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

ii. Le maintien d'une formalité préalable particulière pour les traitements nécessitant l'utilisation du NIR, sauf pour certains d'entre eux

Le Gouvernement propose, en conformité avec le droit européen [(1)], de conserver des formalités préalables quelque peu allégées pour les traitements, par des personnes publiques ou privées, utilisant le NIR, donnée particulièrement signifiante. Le **I** du présent article propose à cette fin une nouvelle rédaction de l'article 22 de la loi de 1978.

(1) Article 87 du règlement général sur la protection des données.

— le principe : une autorisation par « décret-cadre » après avis de la CNIL

Par principe, l'utilisation du NIR devra être autorisée par un « décret-cadre » pris en Conseil d'État, après avis motivé et publié de la CNIL, lequel déterminera la liste des organismes habilités à le faire et les finalités des traitements **(premier alinéa)**.

— les exceptions : l'application du droit commun de l'analyse d'impact pour trois catégories de traitements du NIR

Ne seront toutefois pas concernés par cette exigence d'autorisation trois types de traitements de données parmi lesquelles figure le NIR ou impliquant une consultation du RNIPP (**deuxième à cinquième alinéas**) :

— ceux « *qui ont exclusivement des finalités de statistique publique* » (**1°**) ;

— ceux « *qui ont exclusivement des finalités de recherche scientifique ou historique* » (**2°**) ;

— ceux qui, mis en œuvre par l'État, une personne morale de droit public ou une personne morale de droit privé gérant un service public, visent à mettre à la disposition des usagers de l'administration des téléservices (**3°**).

Les finalités de ces traitements ne justifient pas un encadrement aussi contraignant. Ils relevaient jusqu'alors, respectivement, du régime de la déclaration préalable, de l'autorisation par la CNIL et de l'autorisation par arrêté après avis de celle-ci. À l'avenir, ils seront soumis au droit commun, à savoir la consultation préalable de la CNIL lorsque l'analyse d'impact révèle que le traitement présenterait un risque élevé si le responsable ne prend pas les mesures pour atténuer ce risque.

Des **garanties supplémentaires**, reprenant celles posées par le droit actuel [(1)], sont cependant prévues :

— s'agissant des traitements à des fins de statistique publique et de recherche scientifique ou historique, le NIR doit faire préalablement l'objet d'une opération cryptographique le remplaçant par un code statistique non signifiant, opération qui doit être renouvelée à une fréquence définie par décret en Conseil d'État (**sixième alinéa**) ;

— les traitements à des fins de statistique publique concernés sont seulement ceux qui sont mis en œuvre par le service statistique public, et ne comportent aucune donnée sensible, sous la réserve supplémentaire que le code statistique non signifiant ne puisse être utilisé qu'au sein de l'INSEE (**1° et septième alinéa**) ;

---

(1) Il s'agit de la reprise de la condition prévue, dans le droit actuel, par le I bis *de l'article 22 de la loi de 1978 pour les traitements à finalité de statistique publique et par le 9° du I de l'article 25 de la même loi pour les traitements à finalité de recherche scientifique ou historique.*

— pour les traitements à des fins de recherche scientifique ou historique, il est prévu que l'opération de chiffrement du NIR et, le cas échéant, celle d'interconnexion de deux fichiers ne pourront être opérées par la même personne ni par le responsable du traitement, afin d'éviter qu'une même personne soit destinataire, à la fois, des données identifiantes et des deux bases de données qui y sont associées (**avant-dernier alinéa**).

Les traitements de données de santé utilisant le NIR demeureront soumis aux formalités particulières prévues par le chapitre IX de la loi de 1978 [(1)], à l'exception de ceux mis en œuvre pour répondre, en cas de situation d'urgence, à une alerte sanitaire, qui, dès lors qu'ils utilisent le NIR, devront être autorisés par le même « décret-cadre » (**dernier alinéa**).

iii. La suppression du régime d'autorisation, sauf pour les traitements de l'État portant sur des données génétiques ou biométriques

Le 2° du II et le III du présent article suppriment les formalités préalables d'autorisation telles qu'elles sont prévues par les articles 25 et 27 de la loi de 1978 pour les traitements de données sensibles ou mis en œuvre par l'État ou pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public.

Toutefois, comme l'autorise le droit européen [(2)], le Gouvernement propose de conserver un régime d'**autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL pour les traitements de l'État agissant dans l'exercice de ses prérogatives publiques et portant sur des données génétiques ou biométriques, mis en œuvre aux fins d'authentification ou de contrôle de l'identité des personnes** (**1° du II**).

L'annexe n° 1 à ce rapport permet de disposer d'une vue d'ensemble des évolutions induites par l'adaptation de notre droit aux exigences du règlement européen en matière de formalités préalables.

c. La position de la Commission

La Commission a approuvé l'ensemble de cet article sous réserve, à l'initiative de votre rapporteure, de modifications rédactionnelles et, au III, de l'abrogation de l'article 23 de la loi de 1978 afin de tirer les conséquences de la suppression du régime de déclaration préalable.

*

* *

(1) Voir infra*, le commentaire de l'article 13.*

(2) Article 9, § 4, du règlement général sur la protection des données.

*La Commission **adopte** successivement les amendements rédactionnels CL136, CL137, CL138, CL139 et CL140, l'amendement de clarification CL226 et l'amendement CL207 tendant à corriger une omission, tous de la rapporteure.*

*Puis elle **adopte** l'article 9 **modifié.***

CHAPITRE III
Obligations incombant aux responsables de traitements et sous-traitants

Article 10
(art. 35 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Extension du champ des obligations applicables aux sous-traitants de responsables de traitements de données à caractère personnel

Résumé du dispositif et effets principaux :

Le présent article inscrit dans notre droit l'obligation faite aux sous-traitants par le règlement général sur la protection des données de respecter les mêmes obligations que celles imposées aux responsables de traitements.

L'instauration d'une responsabilité conjointe des responsables de traitements et sous-traitants est l'une des avancées majeures du règlement européen, impliquant d'harmoniser les obligations auxquels ces deux catégories d'acteurs sont soumises.

Dispositions du règlement concernées : articles 24 à 43.

Dernières modifications législatives intervenues :

La question de la sous-traitance des traitements de données personnelles a été introduite à l'article 35 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés lors de la transposition de la directive 95/46/CE du 24 octobre 1995 par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Elle n'a pas fait l'objet de modifications juridiques depuis lors.

Modifications adoptées par la commission des Lois :

Sur proposition de votre rapporteure, la Commission a clarifié le régime des obligations applicables aux sous-traitants selon qu'ils interviennent dans la mise en œuvre d'un traitement relevant du règlement européen, de la directive ou se situant hors du champ de ces deux textes.

1. L'état du droit

Conformément à la directive 95/46/CE du 24 octobre 1995, l'**article 35 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** prévoit que **les données personnelles ne peuvent faire l'objet d'un traitement par un sous-traitant,** défini comme « *toute personne traitant des données à caractère personnel pour le compte du responsable du traitement* », **que « *sur instruction du responsable du traitement* »**.

Plusieurs garanties sont prévues pour encadrer ces opérations :

— le sous-traitant doit présenter des « *garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité* » ;

— le contrat entre le sous-traitant et le responsable du traitement doit indiquer les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et que celui-ci ne peut agir que sur instruction du responsable du traitement ;

— en tout état de cause, les garanties offertes par le sous-traitant ne déchargent pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

2. Le dispositif proposé

a. Le règlement général sur la protection des données

Le règlement 2016/679 du 27 avril 2016 a pour conséquence d'étendre le champ des obligations applicables aux sous-traitants.

Son **chapitre IV** fixe un ensemble d'obligations aussi bien aux responsables de traitements qu'aux sous-traitants susceptibles d'intervenir dans les opérations de traitement :

— la mise en œuvre de **mesures techniques et organisationnelles** appropriées de nature à démontrer que le traitement respecte le règlement et la **protection des droits de la personne concernée**, par exemple à travers l'application d'un code de conduite ou d'un mécanisme de certification approuvés (**articles 24 et 28**) ;

— la **tenue d'un registre des activités de traitement** effectuées, selon le cas, sous leur responsabilité ou pour le compte du responsable du traitement [(1)] (**article 30**) ;

— la **coopération** avec l'autorité de contrôle (**article 31**) ;

---

(1) Cette obligation n'est pas applicable aux entreprises ou organisations de moins de 250 employés, sauf si le traitement « est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9 (…) ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions *».*

— la mise en œuvre de **mesures techniques et organisationnelles** appropriées afin de garantir un **niveau de sécurité adapté au risque** [(1)], par exemple à travers l'application d'un code de conduite ou d'un mécanisme de certification approuvés (**article 32**) ;

— la **notification**, selon le cas, à l'autorité de contrôle ou au responsable de traitement de toute violation de données à caractère personnel (**article 33**) ;

— la **désignation d'un délégué à la protection des données** dès lors que le sous-traitant entre dans le champ des organismes pour lesquels cette désignation est obligatoire (**article 37**).

L'**article 28** prévoit des **obligations spécifiques** pour les sous-traitants. Il s'agit, en premier lieu, de l'obligation de recueillir l'autorisation écrite préalable du responsable du traitement pour le recrutement d'un autre sous-traitant. En second lieu, le contrat liant le responsable du traitement au sous-traitant doit comporter un certain nombre de garanties.

b. Le projet de loi

En cohérence avec les dispositions du règlement général sur la protection des données, le présent article complète l'article 35 de la loi du 6 janvier 1978 par un alinéa qui a pour objet de soumettre les sous-traitants aux obligations telles qu'elles sont fixées par le chapitre IV de ce règlement.

Votre rapporteure observe que les dispositions actuelles de l'article 35, qui restent en vigueur, n'auront désormais vocation à s'appliquer qu'aux traitements ne relevant ni du règlement général sur la protection des données, ni de la directive 2016/679 sur les traitements de données à des fins pénales.

c. La position de la Commission

Sur proposition de votre rapporteure, la Commission a adopté un amendement de rédaction globale de cet article afin de **clarifier le champ des obligations applicables aux sous-traitants** :

— les dispositions actuelles de l'article 35 s'appliqueront aux sous-traitants de responsables de traitements ne relevant ni du règlement général sur la protection des données, ni de la directive relative aux traitements de données à des fins pénales [(2)] ;

---

(1) Telles que la pseudonymisation ou le chiffrement des données, des moyens garantissant la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement ou la disponibilité des données ainsi qu'une procédure testant, analysant et évaluant régulièrement l'efficacité des mesures techniques et organisationnelles.

(2) Sont en pratique concernés les fichiers de souveraineté, les traitements de données de personnes décédées et les traitements exclus par l'article 2 du règlement européen.

— les sous-traitants de responsables de traitements entrant dans le champ du règlement européen devront se conformer aux obligations prévues par ce règlement, auquel il est renvoyé.

Les obligations des sous-traitants de responsables de traitements de données pénales à des fins pénales seront celles mentionnées au nouvel article 70-10 de la loi de 1978, tel qu'il résulte de l'article 19 du projet de loi qui transpose la directive relative aux traitements de données à des fins pénales [(1)].

*
* *

La Commission examine l'amendement CL227 de la rapporteure.

Mme la rapporteure. Cet amendement de clarification porte sur les obligations applicables aux sous-traitants.

La Commission ***adopte*** *l'amendement. L'article 10 est* ***ainsi rédigé****.*

(1) Voir infra*, le commentaire de l'article 19.*

CHAPITRE IV
Dispositions relatives à certaines catégories particulières de traitement

Article 11
(art. 9 de la loi n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés)
Traitements de données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes

Résumé du dispositif et effets principaux :

Le présent article élargit la liste des personnes habilitées à procéder, à des fins autres que la prévention et la répression d'infractions pénales, au traitement de données relatives aux condamnations pénales, aux infractions et aux mesures de sûreté connexes, données d'une particulière sensibilité qui exigent la mise en place de garanties appropriées :

– aux personnes morales de droit privé collaborant au service public de la justice (associations d'aide aux victimes, associations de réinsertion des personnes sous main de justice…) ;

– à certaines personnes aux fins de préparation, de suivi et d'exécution d'une action en justice ;

– et aux réutilisateurs des informations publiques figurant dans les décisions de justice.

Dispositions du règlement concernées : articles 10 et 86.

Dernières modifications législatives intervenues :

Lors de la transposition de la directive 95/46/CE du 24 octobre 1995, la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel avait déjà étendu la liste des personnes autorisées à mettre en œuvre de tels traitements aux personnes morales représentatives des ayants droit en vue de lutter contre les atteintes à la propriété littéraire et artistique.

Modifications adoptées par la commission des Lois :

La Commission a approuvé l'ensemble de cet article. Elle a adopté, à l'initiative de votre rapporteure, des modifications rédactionnelles et un amendement qui prévoit la publication et la motivation de l'avis de la CNIL sur le projet de décret fixant la liste des associations d'aide aux victimes et de réinsertion des personnes condamnées habilitées à traiter des données pénales pour les besoins de leurs missions.

1. L'état du droit

Les traitements de données à caractère personnel relatives aux condamnations pénales, infractions et mesures de sûreté sont régis par l'**article 9 de la loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés [(1)].

Les traitements dont il est question sont ceux qui relèvent de la compétence du règlement 2016/679 et non de celle de la directive 2016/680, c'est-à-dire ceux qui sont mis en œuvre à d'autres fins que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, par tout organisme ou entité – et pas seulement les autorités judiciaires et répressives ou tout autre organisme qui se voit confier l'exercice de l'autorité publique et des prérogatives de puissance publique à ces mêmes fins.

La **nature particulièrement sensible** des données concernées justifie qu'un **nombre réduit et strictement contrôlé de personnes** soit **habilité à les collecter**.

Avant 2004, ces traitements ne pouvaient être mis en œuvre que par les **juridictions**, les **autorités publiques** et les **personnes morales gérant un service public** agissant dans le cadre de leurs attributions légales (**1°**) ainsi que les **auxiliaires de justice** [(2)] pour les stricts besoins de l'exercice de leurs missions (**2°**).

La directive 95/46/CE du 24 octobre 1995 a prévu que de tels traitements ne peuvent être effectués que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues. Toutefois et en tout état de cause, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Lors de la transposition, en 2004, des dispositions de cette directive, le législateur a complété la liste des personnes habilitées à procéder à de tels traitements en y ajoutant les **personnes morales représentatives des ayants droit** en vue de lutter contre les atteintes à la propriété littéraire et artistique [(3)] (**4°**).

---

(1) Avant 2004, ces traitements étaient régis par l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Avocats, avocats au Conseil d'État et à la Cour de cassation, commissaires-priseurs, experts judiciaires, greffiers de commerce, huissiers de justice, notaires, syndics et administrateurs judiciaires.

(3) Sociétés de perception et de répartition des droits d'auteur, des droits des artistes-interprètes et des droits des producteurs de phonogrammes et de vidéogrammes constituées sous forme de sociétés civiles, organismes de défense professionnelle régulièrement constitués et ayant qualité pour ester en justice pour la défense des droits et intérêts dont ils ont la charge.

2. La jurisprudence du Conseil constitutionnel

Le Conseil constitutionnel avait admis la possibilité d'inclure à la liste des personnes habilitées à procéder à de tels traitements les organismes de défense des ayants droit compte tenu de « *l'objectif d'intérêt général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle* » et de l'existence de garanties, comme le fait « *que les données (...) recueillies ne pourront (...) acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire et par rapprochement avec des informations dont la durée de conservation est limitée à un an* » (1).

Avait toutefois été censurée la disposition qui ajoutait les personnes morales victimes d'infractions ou agissant pour le compte de victimes d'infractions pour les besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi. Le Conseil avait considéré qu'une telle disposition pouvait « *affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » et devait dès lors « *comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* » (2). Or, il avait jugé que cette disposition était entachée d'incompétence négative au motif qu'elle était « *ambiguë quant aux infractions auxquelles s'applique le terme de "fraude"* », laissait « *indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction* » et qu'elle ne disait rien « *sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations* » (3).

La déclaration d'inconstitutionnalité était assortie d'une réserve d'interprétation visant à ne pas priver d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne s'agissant des infractions dont elle est victime, et ainsi à ne pas affecter la base légale des traitements mis en œuvre par une personne morale pour suivre les dossiers contentieux relatifs aux infractions dont elle a été victime.

3. Le dispositif proposé

a. Le règlement général sur la protection des données

L'**article 10 du règlement général** sur la protection des données conserve, pour l'essentiel, les exigences posées par la directive 95/46/CE de 1995 pour la mise en œuvre de ces traitements :

---

(1) Décision n° 2004-499 DC du 29 juillet 2004, Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, cons. 13.*

(2) Idem*, cons. 11.*

(3) Idem*, cons. 12.*

— ils ne peuvent être effectués que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union européenne ou par le droit d'un État membre sous réserve de prévoir des garanties appropriées pour les droits et libertés des personnes concernées ;

— l'exigence d'un contrôle de l'autorité publique pour la tenue d'un registre complet des condamnations pénales est maintenue.

Par ailleurs, l'**article 86** de ce règlement autorise les États à prévoir dans leur droit national le traitement et l'accès du public aux « *documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public* », ce qui inclut notamment la **réutilisation des données publiques contenues dans les décisions de justice**.

b. Le projet de loi

Le présent article procède à un **nouvel élargissement du champ des personnes** autorisées à mettre en œuvre de tels traitements.

Le **1°** a pour effet d'inclure dans la liste des traitements concernés ceux mis en œuvre pour le compte de l'autorité publique, comme les hébergements de données sur un serveur.

Les **2° à 4°** ajoutent **trois catégories d'acteurs habilitées à procéder à ces traitements** et prévoient, pour chacune d'elles, des garanties appropriées conformément aux exigences européennes et à la jurisprudence du Conseil constitutionnel.

i. *Les associations d'aide aux victimes et de réinsertion des personnes condamnées*

En premier lieu, sont ajoutées les ***« personnes morales de droit privé collaborant au service public de la justice »***, principalement des associations d'aide aux victimes et de réinsertion des personnes placées sous main de justice (**2°**).

L'usage des données en cause devra être « *strictement nécessaire* » à leur mission et la liste précise de ces personnes sera fixée par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés (CNIL).

ii. Les fichiers « contentieux » ou « précontentieux » mis en œuvre par des organismes privés

En deuxième lieu, le présent article étend la liste aux « *personnes, physiques ou morales, aux fins de leur* ***permettre de préparer et****, le cas échéant,* ***d'exercer et de suivre une action en justice en tant que victime, mise en cause ou pour le compte de ceux-ci et de faire exécuter la décision rendue*** **»** (**3°**).

Sont surtout concernés par cette disposition les traitements mis en œuvre dans le cadre du suivi des dossiers contentieux relatifs aux infractions (traitements des infractions constatées par les commerçants, aux fins de lutte contre la contrefaçon, relatifs aux incivilités des clients, de gestion des procédures de conciliation…) et dont l'existence ne repose sur aucune base légale mais sur la réserve d'interprétation formulée par le Conseil constitutionnel en 2004.

La durée du traitement devra être proportionnée à ces finalités. La communication à un tiers des données traitées, hypothèse qui couvre le cas d'une société mère qui dispose d'un service juridique afin qu'elle puisse traiter ces données pour le compte de ses filiales victimes d'infractions, sera soumise aux mêmes conditions et possible « *dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités* » [(1)].

iii. *La réutilisation des données publiques contenues dans les décisions de justice*

En dernier lieu, sont visés **les « *réutilisateurs des informations publiques figurant dans les jugements et décisions* » rendus par les juridictions administratives et judiciaires (4°)**.

Ces traitements ne pourront être mis en œuvre que sous réserve qu'ils « *n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées* ». Depuis la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, ces jugements et décisions doivent être mis à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées, à condition de faire précéder cette mise à disposition d'une analyse du risque de ré-identification des personnes [(2)].

c. La position de la Commission

La Commission a approuvé l'élargissement des personnes autorisées à traiter des données pénales, sous réserve de modifications rédactionnelles. Elle a également adopté un amendement de votre rapporteure prévoyant la publication et la motivation de l'avis de la CNIL sur le projet de décret qui fixera la liste des associations d'aide aux victimes et de réinsertion des personnes condamnées habilitées à traiter des données pénales pour l'exercice de leurs missions.

*

* *

(1) Cette rédaction diffère, par les garanties qu'elle apporte, de celle qui avait été censurée par le Conseil constitutionnel en 2004, laquelle visait « les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi dans les conditions prévues par la loi *».*

(2) Les conditions d'application et les modalités d'ouverture au public des décisions de justice font l'objet de réflexions de la part du Gouvernement. Dans la perspective de l'application des articles 20 et 21 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, le groupe de travail présidé par M. Loïc Cadiet a remis ses conclusions dans un rapport à la garde des Sceaux rendu le 9 janvier 2018.

La Commission examine l'amendement CL228 de la rapporteure.

Mme la rapporteure. Cet amendement vise à préciser que l'avis de la CNIL sur le projet de décret qui fixera la liste des personnes collaborant au service public de la justice habilitées à traiter les données pénales devra être motivé et publié.

*La Commission **adopte** l'amendement.*

Elle en vient à l'amendement CL87 de Mme Constance Le Grip.

Mme Constance Le Grip. Cet amendement vise à permettre aux entreprises de se conformer aux différentes obligations légales auxquelles elles sont soumises, au-delà de la problématique liée à la protection des données personnelles.

Mme la rapporteure. Vous prévoyez que des organismes privés seraient autorisés à traiter des données pénales sans que leur soient appliquées les garanties appropriées et suffisantes exigées par le règlement européen et le Conseil constitutionnel, compte tenu de la sensibilité particulière de ces données. Avis défavorable.

*La Commission **rejette** l'amendement.*

*Elle **adopte** l'amendement de précision CL141 de la rapporteure.*

*Puis elle **adopte** l'article 11 **modifié**.*

Article 12

(art. 36 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Traitement de données à des fins archivistiques

Résumé du dispositif et effets principaux :

Cet article a pour objet de modifier l'article 36 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés de manière à tirer les conséquences de l'article 89 du règlement européen qui accorde aux traitements à des fins archivistiques, statistique ou de recherche scientifique ou historique des dérogations au cadre général de traitement des données personnelles à la conditions qu'elles s'accompagnent de garanties appropriées pour garantir les droits et les libertés des personnes concernées.

Dispositions du règlement : article 89

Dernières modifications législatives intervenues :

Les dispositions en vigueur sont issues de la loi du 6 août 2004 (1).

Modifications adoptées par la commission des Lois :

La Commission a adopté cet article sans modification.

1. L'état du droit

L'article 36 de la loi du 6 janvier 1978 prévoit que les données à caractère personnel ne peuvent être conservées au-delà de la durée nécessitée par les finalités justifiant leur collecte initiale qu'en vue de traitements à **des fins historiques, statistiques ou scientifiques.**

Le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine, sur la base d'une sélection permettant de déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées.

Ces dernières données et les conditions de leur élimination sont fixées par un accord entre l'autorité qui les a produites ou reçues et l'administration des archives.

Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives sont, par ailleurs, dispensés de formalités préalables devant la CNIL.

La conservation de données à long terme peut également être autorisée pour des traitements ayant d'autres finalités qu'à des fins historiques, statistiques ou scientifiques:

— soit avec l'accord exprès de la personne concernée ou en vertu de ses directives ;

— soit avec l'autorisation de la CNIL ;

— soit dans le cadre de traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé ou de traitements, automatisés ou non, justifiés par l'intérêt public.

(1) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

2. Le dispositif proposé

Le présent article propose, dans un premier temps, d'étendre la faculté de conserver des données au-delà de la durée prévue au regard de la finalité de leur collecte aux traitements à « *des fins archivistiques dans l'intérêt public* » et aligne en cela la rédaction de la loi du 6 janvier 1978 sur celle retenue par le règlement européen (**alinéa 2**).

Il procède également à une coordination visant à supprimer les autorisations préalables délivrées par la CNIL (**alinéa 3**).

Enfin, il complète l'article 36 par des dispositions spécifiques aux traitements réalisés par les services publics d'archives en prévoyant :

— des dérogations aux dispositions de droit commun relatives à la protection des données personnelles pour prendre en compte la spécificité des traitements archivistiques ;

— des garanties appropriées pour les droits et libertés des personnes concernées, conformément aux dispositions de l'article 89 du règlement, grâce à la mise en œuvre de mesures techniques et organisationnelles permettant d'assurer en particulier le principe de minimisation des données. Des mesures ne permettant pas l'identification des personnes ou une démarche de pseudonymisation [(1)] peuvent ainsi être mises en œuvre, sans remettre en cause la finalité du traitement. Ces mesures sont renvoyées, par le présent article, au code du patrimoine ainsi qu'aux autres dispositions législatives ou réglementaires applicables aux archives publiques.

Par ailleurs, il est rappelé que les conditions et garanties appropriées pour ce type de traitements sont assurées dans « *le respect des normes conformes à l'état de l'art en matière d'archivage électronique* ».

*

* *

La Commission ***adopte*** *l'article 12* ***sans modification****.*

(1) Selon l'article 4 du règlement, la pseudonymisation consiste en un « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable *».*

Article 13

(Chapitre IX de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Traitements des données à caractère personnel dans le domaine de la santé

Résumé du dispositif et effets principaux

Cet article a pour objet de regrouper au sein du chapitre IX de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés l'ensemble des dispositions relatives au traitement des données de santé réparties au sein de deux sections présentant pour l'une, les dispositions générales à respecter et, pour l'autre, les dispositions propres aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

Dispositions du règlement et de la directive concernées : articles 9, 13 et 14 du règlement.

Dernières modifications législatives intervenues

L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a permis d'ouvrir davantage l'accès aux données de santé, notamment en faveur de la recherche.

Modifications adoptées par la commission des Lois :

La Commission a apporté des précisions visant à :

– améliorer la cohérence des procédures relatives au traitement des données de santé, conformément aux recommandations de la CNIL ;

– inscrire l'ensemble des dispositions relatives à ces traitements à des fins de recherche, d'étude ou d'évaluation en matière de santé dans la section introduite à cet effet par le présent article.

I. L'ÉTAT DU DROIT

Les conditions d'accès actuelles aux données de santé résultent de la volonté portée par l'article 193 de la loi du 26 janvier 2016 précitée de mieux valoriser ces dernières.

L'objectif poursuivi par le législateur était de permettre, dans le cadre d'un accès plus ouvert et mieux contrôlé aux données de santé, de répondre à la **double exigence de protection effective des données personnelles et d'exploitation des données disponibles** pour permettre notamment des avancées de l'offre de soin et de la recherche médicale.

Il répondait en ce sens aux critiques émises sur le régime antérieur de gestion des données de santé qui comportait de nombreuses limitations d'accès,

entraînant leur sous-exploitation, sans garantir pour autant un niveau de protection suffisant des données personnelles [1].

1. Un cadre de mise à disposition des données de santé rénové

a. La notion de donnée de santé

L'article 4 du règlement européen dont l'objectif est d'uniformiser les définitions des principaux termes utilisés en matière de protection des données au niveau européen considère à son point 15 que les données concernant la santé correspondent aux « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.* » [2]

b. La qualité des bases de données françaises

L'étude d'impact du projet de loi de modernisation de notre système de santé souligne la richesse des bases françaises dont le seul l'ensemble SNIIRAM (système national d'information inter-régimes de l'assurance maladie) et PMSI (programme médicalisé des systèmes d'information) [3] représente « *la plus grande base de données médico-administratives au monde : elle regroupe par an 1,2 milliard de feuilles de soins, 500 millions d'actes médicaux et 11 millions de séjours hospitaliers (en médecine, chirurgie et obstétrique), avec potentiellement (au terme de la montée en charge) une profondeur historique de 14 ans (et même de 20 ans pour l'échantillon généralistes de bénéficiaires et le PMSI).* »

En effet, les bases françaises ont pour caractéristiques de :

— porter sur toute la population, ce qui leur confère une meilleure fiabilité statistique ;

---

(1) Plusieurs travaux ont permis de dresser ce constat, notamment ceux de la Commission « open data en santé » dont le rapport fut remis à la ministre de la santé de l'époque en juillet 2014.

(2) Cette définition est complétée par les dispositions du considérant 35 qui précise que « les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro*. *»*

(3) Cet ensemble contient 16 bases de données différentes dont la durée de conservation diffère selon la nature.

— regrouper les données détaillées sur les consommations de soins en ville et à l'hôpital, notamment tous les traitements médicamenteux prescrits au long cours et toutes les hospitalisations ;

— permettre un chainage (soit des études longitudinales des données des personne à partir d'un évènement de départ) ;

— disposer d'une chronologie précise ;

— présenter des données de qualité du fait notamment de l'exactitude du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) des cartes Vitale et de la saisie automatisée des codes des médicaments.

La disponibilité de telles données rend ainsi d'autant plus regrettable les difficultés d'exploitation qui ont pu exister ou qui perdurent encore aujourd'hui.

c. La nécessité d'un meilleur accès aux bases de données, dans le respect de la protection des données personnelles

Les enjeux de l'accès aux données de santé portent sur différents aspects permettant chacun de contribuer à une amélioration de notre système de santé et de l'offre de soins.

Comme l'a souligné la commission « open data en santé », un meilleur accès à ces données permet, en effet, de :

— **renforcer la démocratie sanitaire** par une meilleure transparence du fonctionnement de notre système de santé, comme le souhaitent notamment les associations de patients et d'usagers qui entendent mieux répondre aux attentes de leurs adhérents et jouer, le cas échéant, leur rôle de lanceurs d'alerte ;

— **permettre l'autonomisation des patients** grâce à de nouveaux services d'information sur l'offre et les parcours de soins de manière à réduire l'asymétrie d'information avec les professionnels de santé et de mieux éclairer leur décision ;

— **accroître l'efficience de l'action publique** par une meilleure évaluation de la qualité des soins et la promotion des bonnes pratiques ;

— **encourager le développement de la recherche** en vue de la production de connaissances utiles à la santé publique ;

— **favoriser l'innovation et rester compétitif** en matière d'accueil d'entreprises du champ de la santé.

L'amélioration de cet accès ne peut toutefois se faire au détriment de la protection des données personnelles et il convient de distinguer l'accès aux

données de santé anonymisées et celle pour lesquelles la réidentification d'une personne est possible.

d. La révision de l'organisation de l'accès aux données de santé

Afin de faciliter l'accès aux données de santé, la loi du 26 janvier 2016 a notamment permis de créer un système national des données de santé (SNDS) qui rassemble les données des bases existantes, ou en cours de constitution, en matière sanitaire et médico-sociale, sous la responsabilité de la caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS).

L'Institut national des données de santé (INDS) est, quant à lui, chargé de veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition garantissant leur protection et facilitant leur utilisation. Cet institut se voit également reconnaître un rôle de guichet unique dans la réception des dossiers de recherche et est amené à se prononcer, à ce titre, sur l'intérêt public que présente une recherche, une étude ou une évaluation.

Données et finalités du SNDS

Conformément à l'article L. 1461-1 du code de la santé publique, le SNDS doit permettre de chainer :

– les données de l'assurance maladie (base SNIIRAM) ;

– les données des hôpitaux (base PMSI) ;

– les causes médicales de décès (base de l'INSERM) ;

– les données relatives au handicap (données de la caisse nationale de solidarité pour l'autonomie) ;

– un échantillon de données en provenance des organismes complémentaires.

Les finalités de la mise à disposition de ces données sont limitativement énumérées au même article et doivent permettre de contribuer à :

– l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;

– la définition, la mise en œuvre et l'évaluation des politiques de santé et de protection sociale ;

– la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;

– l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;

– la surveillance, la veille et la sécurité sanitaires ;

– la recherche, les études, l'évaluation et l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

Par ailleurs, les données du SNDS ne peuvent être utilisées en vue :

– de promouvoir des produits de santé ou cosmétiques en direction des professionnels de santé ou d'établissements de santé ;

– d'exclure un individu présentant un risque de garanties prévues par des contrats d'assurance et de modifier ses cotisations ou ses primes d'assurance.

Pour mémoire, alors que les organismes pouvant tirer un profit des données traitées devaient obligatoirement avoir recours à des organismes de recherche non lucratifs pour procéder à de tels traitements, la loi du 26 janvier 2016 leur reconnait la possibilité d'accéder aux données du SNDS s'ils démontrent que les modalités de mise en œuvre du traitement rendent impossible toute utilisation des données pour l'une des finalités interdites. À défaut, ils doivent avoir recours à un laboratoire de recherche ou à un bureau d'études.

Enfin, les données comprises dans le SNDS sont « pseudonymisées », c'est-à-dire qu'elles ne présentent pas les noms, prénoms, adresse et NIR des personnes concernées. Elles sont également mises à disposition conformément à un référentiel de sécurité assurant la confidentialité et l'intégrité des données, ainsi que la traçabilité des accès et autres traitements.

Si la loi du 26 janvier 2016 a contribué à ouvrir davantage l'accès aux données de santé, celui-ci reste donc fortement encadré au regard de leur sensibilité pour les personnes concernées.

e. Les différentes voies d'accès aux données de santé

La loi du 26 janvier 2016 a permis d'adapter les voies d'accès aux données de santé en fonction de la capacité des utilisateurs de ces données d'identifier ou de réidentifier les personnes concernées.

- *L'accès aux données anonymisées selon une procédure autorisée par la CNIL*

Elle a ainsi introduit, à l'article L. 1461-2 du code de la santé publique, le principe d'une mise à disposition des données de santé publique et gratuite à la condition qu'elles ne puissent donner lieu à l'identification directe ou indirecte des personnes concernées [(1)].

Conformément à l'article 8 de la loi du 6 janvier 1978 précitée, les procédés d'anonymisation doivent au préalable être reconnus conformes par la CNIL qui doit également autoriser le traitement.

- *L'accès aux données présentant un caractère personnel*

Pour les données qui ne sont pas anonymisées, leur accès est encadré par la loi du 6 janvier 1978 précitée de manière à assurer que :

— elles sont collectées et traitées de manière loyale et licite ;

(1) « Les données du système national des données de santé qui font l'objet d'une mise à la disposition du public sont traitées pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées y est impossible. Ces données sont mises à disposition gratuitement. La réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées. »

— leur collecte répond à des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;

— elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

— elles sont exactes, complètes et, si nécessaire, mises à jour. Dans le cas contraire, les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

— elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Par ailleurs, le traitement de telles données doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

— respecter une obligation légale incombant au responsable du traitement ;

— assurer la sauvegarde de la vie de la personne concernée ;

— exécuter d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

— exécuter, soit un contrat auquel la personne concernée est partie, soit des mesures précontractuelles prises à la demande de celle-ci ;

— réaliser l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

En second lieu, ce cadre général est précisé pour les données de santé selon les traitements à réaliser. Ainsi, l'accès aux données personnelles contenues dans le SNDS, ne peut être autorisé, selon l'article L. 1461-3 code la santé publique, que pour permettre des traitements :

— **nécessaires à l'accomplissement des missions des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public compétents**. Ces organisations, listées par décret en conseil d'État, pris après avis de la CNIL, peuvent pour accomplir leurs missions accéder à certaines données de manière permanente [(1)] ;

---

(1) Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ». À titre d'exemple, cet accès dérogatoire est prévu notamment pour l'agence Santé publique France, l'Agence nationale de sécurité du médicament et des produits de santé, la Haute Autorité de santé, l'INSERM, l'agence de biomédecine ou encore les Agences régionales de santé.

— **à des fins de recherche, d'étude ou d'évaluation** contribuant à une des finalités du SNDS et répondant à un motif d'intérêt public.

Ce dernier accès a été profondément révisé par la loi du 26 janvier 2016 au sein du chapitre IX de la loi du 6 janvier 1978.

Les demandes d'accès doivent être déposées devant l'INDS qui en assure le traitement en lien avec deux comités différents, soit le comité de protection des personnes (article L. 1123-6 du code de la santé publique) et le comité d'expertise pour les recherches n'impliquant pas la personne humaine (CEREES), dont le rôle est de donner à la CNIL **un avis sur la cohérence entre la finalité de l'étude proposée, la méthodologie présentée et le périmètre des données auxquelles il est demandé accès.**

Cette expertise doit permettre de faciliter l'examen des demandes par la CNIL et de réduire les délais d'instruction.

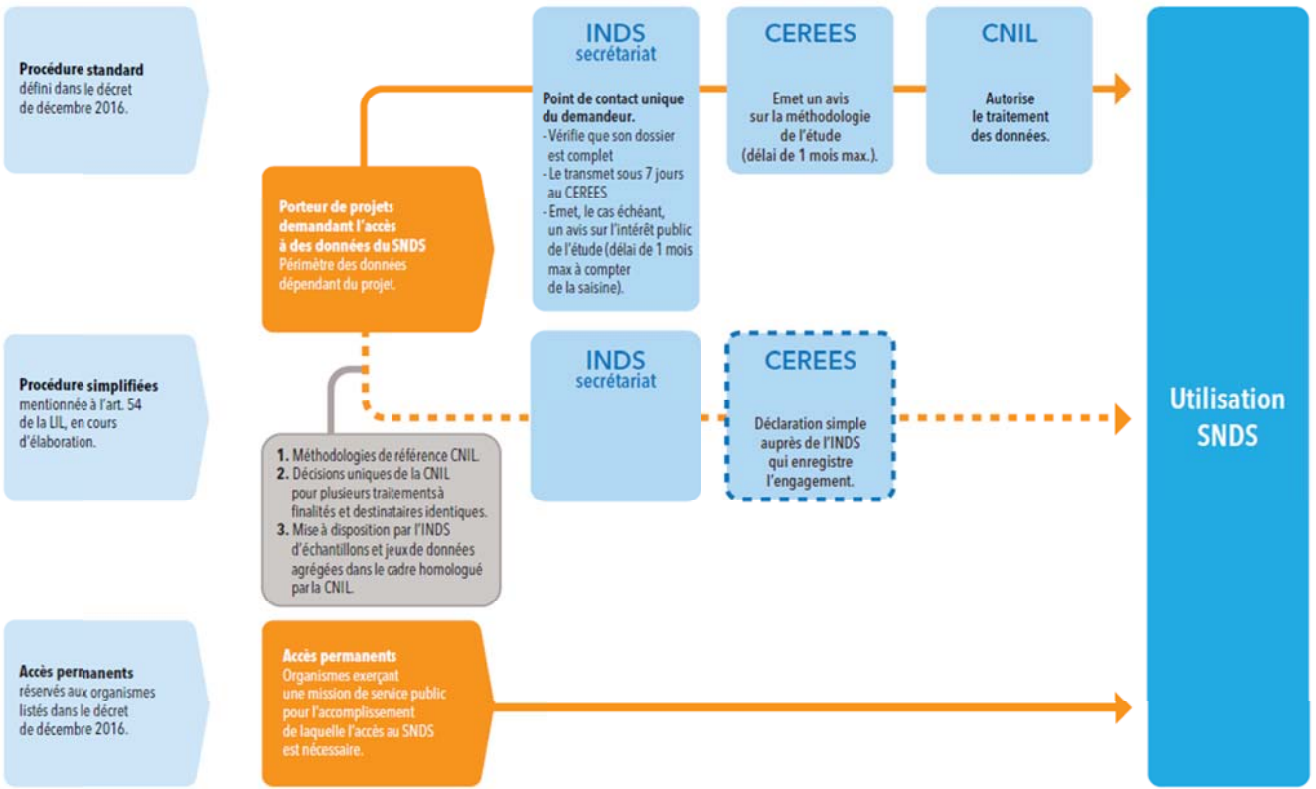
Par ailleurs, l'article 54 de la loi du 6 janvier 1978 prévoit trois procédures d'accès simplifiées :

— un demandeur qui s'engage à se conformer à une **méthodologie de référence** définie par la CNIL et se déclare comme tel peut accéder directement aux données ;

— des **autorisations uniques** peuvent être délivrées par la CNIL à des organismes réalisant plusieurs traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques ;

— des **jeux de données agrégées** ou des échantillons peuvent être mis à disposition par l'INDS lorsqu'ils sont issus des traitements des données de santé à caractère personnel pour des finalités et dans des conditions reconnues conformes à la loi du 6 janvier 1978 par la CNIL, dans des conditions que cette dernière aura préalablement homologuées.

Les schémas d'accès aux données du SNDS



2. Une dispersion des textes relatifs aux données de santé

Les dispositions encadrant l'accès aux données de santé sont principalement réparties entre le code de la santé publique et la loi du 6 janvier 1978, mais d'autres dispositions se trouvent également dans le code de la sécurité sociale ou le code de la recherche.

Selon l'étude d'impact du présent article, il en résulte des difficultés d'interprétation entre l'État et la CNIL, ainsi que des entraves à l'accès aux données.

Le Gouvernement souligne à ce titre que :

— les autorisations d'accès sont délivrées au terme de délais trop longs qui ne sont pas compatibles avec les besoins des acteurs économiques [(1)] ;

— des données peuvent être rendues accessibles dans des conditions « *susceptibles de porter atteinte à la vie privée des citoyens, lesquels s'avèrent le plus souvent insuffisamment informés de l'utilisation de leurs données personnelles.* »

Par ailleurs, les nouvelles obligations et missions confiées à la CNIL pourraient entraîner un allongement des délais au regard des moyens dont elle dispose, tandis que les procédures simplifiées actuellement en vigueur sont encore en cours de développement.

II. LE DISPOSITIF PROPOSÉ

Le présent article propose une réécriture intégrale du chapitre IX, désormais relatif à l'ensemble des traitements de données à caractère personnel dans le domaine de la santé.

Il présente toutefois des difficultés de rédaction qui ont été soulignées par la CNIL ainsi que par d'autres acteurs du secteur de la santé auditionnés par votre rapporteure, auxquelles il convient de répondre pour assurer la sécurité juridique des responsables de traitement, le respect de la protection des données des personnes concernées, et ne pas constituer un frein à l'innovation dans ce domaine.

---

(1) La prorogation du délai de deux mois par la CNIL serait systématique et pourrait aller jusqu'à des délais pouvant atteindre 18 mois, le silence de la CNIL valant refus.

1. Les dispositions générales encadrant le traitement des données de santé

Une première section introduite au sein de ce chapitre a pour objet de regrouper les dispositions générales s'appliquant aux traitements de données de santé.

a. Le champ d'application

L'article 53, dans la rédaction proposée, liste en préalable les exceptions à l'application de ces dispositions (**alinéa 6**). Ne seraient ainsi pas concernés :

— les traitements portant sur des données sensibles définies à l'article 8 de la même loi [(1)], à l'exception des traitements à finalité statistiques, des traitements des données de santé justifiés par l'intérêt public et de certains traitements mis en place par les employeurs ou les administrations dans le cadre de l'activité de leurs salariés ou de leurs agents (**alinéa 7**) ;

— les traitements permettant d'effectuer des études à partir des données recueillies aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif (**alinéa 8**) ;

— les traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie (**alinéa 9**) ;

— les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique (**alinéa 10**) ;

— les traitements effectués par les agences régionales de santé, par l'État et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article (**alinéa 11**).

Ce champ est sensiblement le même que celui en vigueur dans l'actuel chapitre IX encadrant le traitement de données de santé en matière de recherche, d'étude et d'évaluation. De nombreuses dispositions relatives à ces traitements demeurent donc prévues par d'autres sources de droit.

b. Les conditions d'autorisation de ces traitements

Les conditions générales d'autorisation des traitements de santé reprennent également, en grande partie, celles prévues par le droit en vigueur pour les traitements à des fins de recherche, d'étude et d'évaluation.

---

(1) Se reporter au commentaire de l'article 7 du présent projet de loi.

L'article 54 précise, conformément au principe rappelé par le règlement européen, que les traitements de données de santé ne peuvent être mis en œuvre qu'en considération de la **finalité d'intérêt public** qu'ils présentent (**alinéa 12**).

Par ailleurs, il prévoit que la CNIL établit des référentiels et des règlements types s'appliquant à ces traitements, comme le prévoit l'article 1er du présent projet de loi, en précisant toutefois que ces derniers donnent lieu à une concertation avec l'Institut national des données de santé et des organismes publics et privés représentatifs des acteurs concernés (**alinéa 13**).

Cette précision a suscité des interrogations lors des auditions réalisées, l'INDS intervenant plus spécialement dans l'accompagnement des acteurs en matière de recherche, d'étude et d'évaluation (selon le 3° de l'article L. 1462-1 du code de la santé publique) (1).

Ces référentiels peuvent porter, le cas échéant, sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée (**alinéa 15**).

Les traitements conformes à ces référentiels et règlements types pourront être mis en œuvre à la suite d'une déclaration préalable à la CNIL (**alinéa 14**).

En cas de non-conformité de ces traitements à ces règles, le régime d'autorisation préalable par la CNIL s'applique (**alinéa 16**).

Par ailleurs, le régime d'autorisation unique d'ores et déjà mis en œuvre par la CNIL est maintenu. Ainsi, la commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques (**alinéa 18**).

c. Les délais de décision de la CNIL

Si les délais dont disposent la CNIL pour se prononcer ne sont pas modifiés, son silence à leur expiration ne vaut plus refus mais acceptation, sauf dans le cas où l'autorisation fait l'objet d'avis préalables et que ces avis ne sont pas expressément favorables (**alinéas 19 et 20**).

Dans son avis sur le projet de loi, le Conseil d'État « *observe que les conséquences de ce régime de décision implicite sur les moyens humains et matériels de la CNIL n'ont pas fait l'objet d'une analyse de la part du Gouvernement qui devra veiller à ce que cette commission dispose des moyens de prendre effectivement position au regard de l'importance et du nombre de ces traitements.* » (2)

---

(1) Comme cela est déjà le cas, l'INDS pourra, par ailleurs, être saisi par la CNIL ou le ministre chargé de la santé, ou se saisir, dans des conditions définies par décret en Conseil d'État, sur le caractère d'intérêt public que présente le traitement (alinéa 17).

(2) Avis n° 393836 du 7 décembre 2017 sur un projet de loi d'adaptation du droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La CNIL appelle également à cette même prudence en soulignant l'importance du nombre « *de dossiers qui lui est soumis (plus de 700 demandes d'autorisations reçues en 2017) et, surtout, leur sensibilité.* » (1)

d. Les autres dispositions générales, notamment en termes d'information des personnes concernées

Les autres dispositions de la première section proposent également une réécriture des dispositions prévues au chapitre IX pour les traitements à des fins de recherche, d'étude ou d'évaluation de manière à les étendre à tout traitement portant sur des données de santé :

— l'article 55 reprend les dispositions dérogatoires prévues par le droit en vigueur en cas d'alerte sanitaire (**alinéas 21 à 23**) ;

— l'article 56 reprend, pour sa part, les dispositions prévues en cas de transferts de données par des membres des professions de santé à un responsable de traitement (**alinéas 24 à 27**) ;

— l'article 57 rappelle les conditions dans lesquelles une personne peut s'opposer à ce que des données la concernant fassent l'objet de la levée du secret professionnel (**alinéas 28 à 30**) ;

— l'article 58 concerne l'obligation d'information individuelle obligatoire des personnes auprès desquelles sont recueillies les données personnelles (**alinéas 31 et 32**) ;

— l'article 59 traite des conditions d'information des titulaires de l'autorité parentale et personnes assimilées, en distinguant des obligations générales et des obligations réservées aux traitements à fins de recherche, d'étude ou d'évaluation. Elles reprennent pour l'essentiel le droit en vigueur, en maintenant notamment la fixation à 15 ans de l'âge de consentement des mineurs à un traitement de leurs données personnelles de santé (**alinéas 33 à 36**) (2). **Des coordinations sont toutefois à prévoir** avec les dispositions du code de la santé publique en la matière ;

— l'article 60 prévoit enfin qu'une information relative aux dispositions de ce chapitre doit notamment être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données personnelles en vue d'un traitement (**alinéa 37**).

---

(1) Délibération n° 217-299 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 6 janvier 1978.

(2) Pour mémoire, cet âge a été fixé par l'article 56 de la loi du 7 octobre 2016 pour une République numérique.

2. Les dispositions spécifiques aux traitements aux fins de recherche, d'étude et d'évaluation

Les dispositions des articles 61 à 63, dans la rédaction proposée, reprennent les conditions générales d'autorisation prévues à l'article 54 (**alinéas 40 à 42**) en précisant toutefois que cette autorisation est donnée après avis :

— du comité compétent de protection des personnes pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine (**alinéa 44**);

— du CEREES pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine (**alinéa 45**).

Par ailleurs, il est précisé que les dossiers présentés, à l'exclusion des recherches impliquant la personne humaine, sont déposés auprès d'un secrétariat unique assuré par l'INDS, qui assure leur orientation vers les instances compétentes (**alinéa 46**).

3. La nécessité de clarifier la rédaction du présent article

Dans son avis sur le projet de loi, la CNIL a fait part de fortes interrogations « *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 en la matière.* »

L'INSERM et l'INDS ont également souligné le manque de clarté de la rédaction proposée lors de leur audition par la rapporteure pour avis de la commission des affaires sociales.

Certaines dispositions prévues dans la première section du chapitre IX n'ont ainsi pas vocation à s'appliquer à tous les traitements de santé et il conviendrait de préciser la rédaction de l'article en ce sens.

Par conséquent, la Commission a apporté des précisions visant à :

– améliorer la cohérence des procédures relatives au traitement des données de santé, conformément aux recommandations de la CNIL, tout en s'assurant que les procédures d'accès à ces données ne soient pas alourdies pour les personnes concernées ;

– inscrire l'ensemble des dispositions relatives à ces traitements à des fins de recherche, d'étude ou d'évaluation en matière de santé dans la section introduite à cet effet par le présent article.

*

* *

La Commission ***adopte*** *successivement les amendements de cohérence CL142 et CL143, l'amendement rédactionnel CL144, l'amendement de cohérence CL208, les amendements de précision CL145, CL146 et CL147 et l'amendement de coordination CL258 de la rapporteure.*

Puis elle examine l'amendement CL257 de la rapporteure.

Mme la garde des Sceaux. Le Gouvernement est défavorable à cet amendement.

D'une part, l'exposé sommaire évoque le consentement, alors que l'alinéa que l'amendement vise à supprimer porte sur l'information.

D'autre part, l'information sur le traitement des données est de nature à porter à la connaissance du patient la pathologie dont il est atteint, en contradiction avec le droit pour la personne de rester dans l'ignorance prévu à l'article L. 1112-2 du code de la santé publique, dès lors que l'on précise la finalité du traitement.

Cet alinéa constitue une précision qu'il convient de conserver.

Mme la rapporteure. La personne a le droit d'être informée et de dire si elle donne son consentement, même si elle a par ailleurs exprimé qu'elle souhaitait rester dans l'ignorance et ne pas avoir connaissance de la cause de sa pathologie. Je retire cet amendement, afin de pouvoir en modifier la rédaction d'ici l'examen en séance publique.

L'amendement est ***retiré.***

La Commission ***adopte*** *successivement l'amendement rédactionnel CL149, l'amendement de précision CL265, l'amendement de coordination CL256 et l'amendement de cohérence CL150 de la rapporteure.*

Puis elle ***adopte*** *l'article 13* ***modifié.***

Après l'article 13

La Commission est saisie de l'amendement CL12 de Mme Blandine Brocard.

M. Éric Bothorel. Cet amendement vise à définir la manière selon laquelle un consentement au traitement des données personnelles peut être obtenu et à empêcher les contournements de l'actuelle législation par les responsables de traitement.

Introduite par l'article 22 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, la définition du consentement doit être précisée car elle fait l'objet de nombreux abus et de contournements. Le consentement peut ainsi

être extorqué de manière déloyale en masquant la possibilité de le refuser ou en recourant à différentes formulations ou artifices techniques.

L'amendement vise à intégrer la définition du consentement donnée par la CNIL et le G29 : il doit être sans ambiguïté et donné librement ; le refus de consentement ne doit pas empêcher l'accès à un service si celui-ci ne nécessite pas de consentement.

Mme la rapporteure. Les principes du consentement sont bien définis au niveau européen dans le Règlement général sur la protection des données (RGPD), qui sera d'application directe à compter du 25 mai prochain. Il appartiendra au Gouvernement, par voie d'ordonnance, de procéder à cette recodification. Nous pourrons voir s'il est nécessaire d'apporter des précisions d'ici l'examen du texte en séance publique, mais pour l'heure, je vous prie de bien vouloir retirer l'amendement.

M. Éric Bothorel. Par esprit constructif, et compte tenu de la proposition de la rapporteure, je retire l'amendement.

L'amendement CL12 est ***retiré.***

CHAPITRE V
Dispositions particulières relatives aux droits des personnes concernées

Article 14 A (nouveau)
(art. 7 *bis* [nouveau] de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Consentement des mineurs

Résumé du dispositif et effets principaux :

Cet article abaisse de 16 à 15 ans l'âge, fixé par le règlement européen, à partir duquel un mineur peut consentir seul au traitement des données qui le concernent, prévoit le double consentement des parents et du mineur en-dessous de cet âge et soumet les responsables de traitements à une obligation d'information des mineurs dans des termes adaptés à leur âge.

Il a pour objet de mieux concilier l'exigence de protection des enfants sur internet et la nécessité de mieux accompagner les mineurs dans l'apprentissage des usages numériques.

Disposition du règlement concernée : article 8.

1. Le droit en vigueur

En l'état du droit, la loi française est silencieuse sur la question du traitement des données personnelles des mineurs.

Toutefois, dans la pratique, les réseaux sociaux sont généralement interdits aux mineurs de moins de 13 ans, seuil qui a été retenu par la loi américaine dite « COPPA » [(1)] à laquelle se sont conformés les grands acteurs du numérique, souvent américains, qui prohibent l'inscription à leurs sites des mineurs de moins de 13 ans ou imposent un consentement parental préalable.

2. Le dispositif proposé

a. Le règlement général sur la protection des données

Le règlement européen sur la protection des données comporte des dispositions spécifiques destinées à protéger les enfants. En particulier, son article 8 fixe à **16 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données « *en ce qui concerne l'offre directe de services de la société de l'information* »** (sont notamment concernés les réseaux sociaux, les plateformes d'échanges en ligne, les moteurs de recherche ou les services d'annuaires et de référencement) mais permet aux États d'abaisser ce seuil jusqu'à 13 ans.

b. Le projet de loi initial

Le Gouvernement n'ayant pas souhaité utiliser la marge de manœuvre laissée par le règlement, le projet de loi ne comportait aucune disposition spécifique relative au consentement des mineurs : c'est donc l'âge de 16 ans qui devait s'appliquer. Cette situation était conforme à la position défendue par la France lors des négociations européennes.

Il n'existe cependant pas, sur cette question, de consensus européen puisque d'autres pays ont fait le choix d'abaisser cet âge à 13 ans (Irlande, République tchèque, Royaume-Uni), 14 ans (comme s'apprête à le faire l'Espagne) ou 15 ans (Croatie et Grèce), alors que l'Allemagne et le Luxembourg ont maintenu le seuil de 16 ans.

c. La position de la Commission

Avec un avis de sagesse du Gouvernement, **la Commission a choisi de recourir à la marge de manœuvre laissée par le règlement et a adopté un amendement de votre rapporteure créant un nouvel article 7 *bis* au sein de la loi « Informatique et libertés » qui abaisse ce seuil à 15 ans**.

Ce choix a été conforté par les auditions conduites par votre rapporteure sur ce sujet, au terme desquelles un relatif consensus des associations protectrices des intérêts de l'enfant et des acteurs du numérique s'est dégagé autour d'un abaissement raisonnable de l'âge du consentement.

---

(1) Children's Online Privacy Protection Act.

Votre rapporteure n'ignore ni les difficultés liées à la fixation d'un seuil suffisamment protecteur pour les mineurs et réaliste eu égard aux pratiques numériques actuelles, ni la sensibilité de cette question par nature spécifique à chaque adolescent et qui doit, malgré tout, être réglée par une norme générale. Elle observe toutefois que l'âge de 15 ans correspond souvent à l'entrée au lycée, qui constitue une étape importante dans l'acquisition d'une maturité suffisante. Ce seuil est aussi celui fixé par la loi pour une République numérique de 2016 et repris à l'article 13 du projet de loi pour qu'un mineur puisse s'opposer à l'accès de ses parents aux données de santé qui le concernent. De surcroît, il serait pour le moins paradoxal d'exiger qu'un mineur ait 16 ans pour s'inscrire sur un réseau social alors qu'il est réputé pouvoir librement disposer de son corps et de sa sexualité à l'égard d'un majeur à compter de l'âge de 15 ans, seuil retenu par le code pénal pour établir la majorité sexuelle [(1)]. Enfin, l'âge de 16 ans est généralement retenu par notre droit pour autoriser le mineur à accomplir seul des actes qui engagent bien davantage qu'une inscription sur un réseau social [(2)].

Le nouvel article 7 *bis* ainsi créé dispose que le « *mineur âgé de moins de quinze ans peut être autorisé par le ou les titulaires de l'autorité parentale (…) à consentir seul* » au traitement de ses données. Autrement dit, **un double consentement de l'enfant et de ses parents sera exigé pour les mineurs de moins de 15 ans**.

Enfin, il prévoit que **les responsables de traitements devront faire preuve de pédagogie dans la manière dont ils communiquent des informations à un mineur** afin que ces derniers comprennent parfaitement les conséquences de leur choix, en rédigeant « *en des termes clairs et simples, aisément compréhensibles par le mineur, toute information et communication relatives au traitement qui le concerne* ». Cette obligation pourra s'inscrire plus généralement dans une démarche d'encouragement des acteurs numériques au respect des règles protectrices des enfants sur internet, par exemple par la labellisation par la CNIL de produits et de procédures telle qu'elle est prévue au *c)* du 3° de l'article 11 de la loi de 1978.

*

* *

La Commission est saisie de l'amendement CL234 de la rapporteure.

Mme la rappporteure. La question de l'âge du consentement des mineurs a été longuement abordée lors de la discussion générale. Cet amendement vise à l'abaisser à 15 ans, âge où le mineur entre généralement au lycée et où sa maturité

---

(1) L'infraction d'atteinte sexuelle réprimée par l'article 227-25 du code pénal est constituée par « le fait, par un majeur, d'exercer sans violence, contrainte, menace ni surprise une atteinte sexuelle sur la personne d'un mineur de quinze ans *».*

(2) Pour accomplir les actes d'administration nécessaires à la création et à la gestion d'une entreprise individuelle à responsabilité limitée, faire un testament ou réclamer la nationalité française dans le cas des mineurs étrangers.

lui permet en principe de maîtriser les usages sur internet. Cela permettrait en outre d'homogénéiser les textes, puisque le même âge constitue le seuil de consentement en matière de sexualité ou d'opposition à l'accès des parents aux données de santé du mineur.

M. Rémy Rebeyrotte. Il existe un certain consensus des groupes sur cet âge, qui correspond au moment où l'on quitte la puberté et l'adolescence pour entrer, comme jeune adulte, dans une autre phase de construction. Mme la ministre l'a rappelé hier, d'autres débats mettent en avant cet âge, reconnu comme celui d'une certaine forme de maturité avant la majorité : il aurait semblé pour le moins étonnant que la maturité reconnue du mineur dans le domaine sexuel survienne avant sa maturité numérique supposée !

Nous avons auditionné de nombreux acteurs, des associations qui défendent la place de l'enfance dans le numérique comme des grands groupes du numérique. Ainsi que l'a souligné le représentant d'un opérateur, l'âge de 15 ans présente l'avantage d'être plus distinct, car plus éloigné que celui de 16 ans, de la majorité. Il nous a semblé que la fixation du seuil à 15 ans pourrait satisfaire la plupart d'entre nous.

Mme Christine Hennion. Comme je l'ai souligné dans mon rapport, les usages ont beaucoup évolué et les enfants accèdent à un âge bien plus jeune aux réseaux sociaux . D'autre part, les plateformes et les entreprises ne seront pas capables de vérifier si les personnes qui s'inscrivent à leur service ont l'âge requis et, *a fortiori*, si les parents ont donné leur accord éclairé.

Je propose que nous discutions à nouveau de ce sujet dans l'hémicycle et déposerai à cet effet un amendement visant à abaisser à 13 ans l'âge de consentement, ainsi que le permet le règlement européen.

Mme la garde des Sceaux. Sans reprendre l'argumentaire que j'ai développé hier, je veux dire à M. Rebeyrotte que l'âge de la maturité sexuelle a peu à voir avec l'âge de la maturité numérique ! J'entends toutefois le souci de cohérence qui motive cet amendement et m'en remets à votre sagesse.

La Commission ***adopte*** *l'amendement.*

L'article 14 A est ***ainsi rédigé.***

Article 14
(art. 10 de la loi n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés)
Décisions administratives automatisées

Résumé du dispositif national et effets principaux :

Le présent article propose d'ouvrir plus largement la possibilité pour l'administration de recourir à des décisions automatisées (prises sur le fondement d'un algorithme), dans le seul champ des décisions administratives individuelles (et non pour toute décision ayant un effet significatif sur la personne), à la condition d'offrir d'importantes garanties en contrepartie, en matière d'information pleine et entière des personnes, de maîtrise des traitements, de droit au recours et de données traitées (exception des données dites « sensibles » de ce cadre).

Dispositions européennes : article 22 du règlement (UE) 2016/679

Dernières modifications législatives intervenues :

L'article 10 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés proscrit le profilage automatique pour les décisions de justice et précise qu'aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le « seul » fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a prévu des mesures assurant la transparence des décisions individuelles prises sur le fondement d'un traitement algorithmique à travers la création d'une obligation générale de publication en ligne des règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles, et l'obligation pour l'administration d'informer l'usager, par une mention explicite dans la décision, que ladite décision a été prise sur le fondement d'un tel traitement et qu'il peut en demander les règles, y compris leur application dans son cas particulier.

Modifications adoptées par la commission des Lois :

Sur proposition de la rapporteure, la Commission a clarifié les exceptions au principe selon lequel aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données et les garanties minimales à respecter dans ces cas-là.

1. L'état du droit

L'encadrement législatif de l'utilisation des algorithmes et des droits des personnes à l'égard des traitements des données à caractère personnel est régi par

la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

— à l'article 10, qui proscrit la prise de décision à l'égard d'une personne 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. Toutefois, le dernier alinéa de cet article précise que ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions s'inscrivant dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée ;

— à l'article 39, qui accorde à toute personne physique justifiant de son identité le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir les informations permettant de connaître et de contester la logique qui sous–tend le traitement automatisé en cas de décision prise sur le fondement de celui–ci et produisant des effets juridiques à son égard. Les informations communiquées à la personne ne doivent toutefois pas porter atteinte au droit d'auteur.

En complément de la loi du 6 janvier 1978, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a prévu des mesures assurant la transparence des décisions individuelles prises sur le fondement d'un traitement algorithmique.

L'article L. 312-1-3 du code des relations entre le public et l'administration prévoit une obligation générale pour les administrations de publication en ligne des règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles.

L'article L. 311-3-1 du même code a créé, parallèlement, un régime d'information individuelle. L'administration doit informer l'usager, par une mention explicite dans la décision, que ladite décision a été prise sur le fondement d'un traitement algorithmique et qu'il peut en demander les règles, y compris leur application dans son cas particulier ; les règles définissant le traitement algorithmique ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande.

L'article R. 311-3-1-3 de ce code précise les informations qui, dans cette hypothèse, doivent être communiquées à l'intéressé :

« 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2° Les données traitées et leurs sources ; 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; 4° Les opérations effectuées par le traitement ».

Cette logique de transparence permet de comprendre et d'auditer le traitement et, grâce aux informations obtenues au titre des droits de l'intéressé mentionnés plus haut, de rejouer les opérations effectuées par le traitement.

2. Le dispositif proposé

a. Le règlement général sur la protection des données

L'article 22 du règlement (UE) 2016/79 fixe les règles relatives à l'utilisation d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage.

Le principe (point 1) est que la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Néanmoins, ce principe ne s'applique pas (point 2) lorsque la décision :

— est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable de traitement (a) ;

— est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable de traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée (b) ;

— est fondée sur le consentement explicite de la personne concernée (c).

Dans les cas visés par les points a) et c) le responsable de traitement doit (point 3) mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable de traitement, d'exprimer son point de vue et de contester la décision.

À l'inverse, le règlement offre une marge de manœuvre en droit national (point 2. b) pour autoriser la prise de décision individuelle automatisée, à condition de prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée.

Le dernier alinéa de l'article 22 du règlement (point 4) prévoit néanmoins que les décisions individuelles résultant d'un traitement algorithmique ne peuvent être fondées sur les catégories de données prévues à l'article 9 du règlement, c'est-à-dire les données sensibles (données biométriques, génétiques, de santé, ethniques, politiques, syndicales, vie sexuelle, religieuse, philosophique), sauf si la personne y consent ou que le traitement est nécessaire pour des motifs d'intérêt public important.

Le considérant 71 du règlement apporte quelques éclairages sur le sens de l'article 22 du règlement sans toutefois définir précisément les mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée nécessaires pour autoriser la prise de décision individuelle automatisée (point 2 b) :

« *(71) La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision, qui peut comprendre une mesure, impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques la concernant ou qui, de façon similaire, l'affecte de manière significative, tels que le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine. Ce type de traitement inclut le « profilage » qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative.*

Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement, ou nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée a donné son consentement explicite. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant.

Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entrainent des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, et sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de

peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatises fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques. »

b. Le projet de loi

L'essor de l'intelligence artificielle pose directement la question de l'automatisation de la prise de décisions parfois très importantes pour le destin des individus. Entre une interdiction de principe de toute prise de décision automatisée sur le seul fondement d'un traitement de données à caractère personnel et la volonté d'acteurs privés mais aussi, de plus en plus, d'acteurs publics d'ouvrir la voie à une automatisation totale et massive de la prise de décision dans certains domaines, une voie raisonnable doit être établie, permettant le développement de l'automatisation de la prise de décision, gage d'une administration modernisée, tout en apportant à l'individu et à la collectivité des garanties substantielles.

Le présent article entend poursuivre cet objectif en modifiant l'article 10 de la loi n° 78-17 pour transposer les a) et c) du point 2 de l'article 22 du règlement général sur les données personnelles (alinéas 1 à 4) et, plus particulièrement, utiliser la marge de manœuvre offerte par le b) du point 2 de ce même article afin d'autoriser la prise de décision individuelle administrative automatisée – c'est à dire prises sur le seul fondement d'un algorithme.

Il prévoit, au titre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée (alinéas 5 à 7), les obligations suivantes :

— l'interdiction que le traitement porte sur des données mentionnées au I de l'article 8 de la loi n° 78-17, c'est à dire des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ;

— le respect de l'article L. 311-3-1 du code des relations du public et de l'administration selon lequel l'administration doit informer l'usager, par une mention explicite dans la décision, que celle-ci a été prise sur le fondement d'un traitement algorithmique et qu'il peut en demander les règles, y compris leur application dans son cas particulier ;

— l'obligation, pour le responsable de traitement, de « *s'assurer de la maîtrise du traitement algorithmique et de ses évolutions* ». En conséquence, le présent article supprime le troisième alinéa de l'article 10 qui prévoyait 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 » ;

— enfin, les décisions en cause doivent pouvoir faire l'objet d'un recours administratif.

Dans son avis sur le présent projet de loi, le Conseil d'État a insisté sur le fait que « *le responsable du traitement est tenu de se donner les moyens de maîtriser l'algorithme et de documenter, notamment à destination de l'autorité de contrôle, les actions entreprises à cette fin* ».

Selon le Conseil d'État, « *il est en effet essentiel, alors même qu'il n'est plus nécessaire que l'action humaine s'interpose entre le traitement et la prise de décision, de garantir à tout instant une maîtrise humaine complète des algorithmes, comportant notamment la capacité d'interrompre le fonctionnement du traitement, notamment lorsque ceux-ci sont dotés de capacités d'apprentissage leur permettant de modifier leur logique de fonctionnement sans une démarche humaine préalable de validation. Le rappel de ce principe n'est toutefois conçu que comme un premier pas vers la définition d'un régime plus complet du contrôle des algorithmes, y compris au-delà du champ des décisions administratives individuelles, qui apparaît de plus en plus nécessaire* » (1).

La Commission nationale Informatique et Libertés (CNIL) est elle-aussi soucieuse d'améliorer les garanties entourant le renversement du principe jusqu'alors posé par l'article 10 de la loi n° 78-17. Elle souligne, dans son avis sur le présent projet de loi, 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* » (2).

Or, la CNIL estime que le dispositif proposé *« 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*

---

(1) Voir l'avis sur le site : http://www.assemblee-nationale.fr/15/pdf/projets/pl0490-ace.pdf.

(2) Voir l'avis sur le site : https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf.

prévoir elle-même l'ensemble des garanties, la formulation du projet de loi n'apparait pas satisfaisante en l'état ».

En outre, la CNIL regrette « *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 maitrise 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* ».

Il faut en effet reconnaître que la rédaction du présent article ne tient pas compte de la diversité des traitements algorithmiques mis en œuvre par les autorités administratives. Il peut en effet s'agir :

— de simples algorithmes d'application stricte de la loi ou de constatation d'états objectifs, dont le résultat n'est pas soumis à variation, comme dans le cadre du dispositif « Admission-post-bac » (APB) ou de l'algorithme de calcul de l'impôt sur le revenu ou d'affectation du RSA par exemple ;

— d'algorithmes à visée de prévention ou de détection, reposant sur le profilage et où le résultat n'est qu'une probabilité, comme dans le cas des traitements de lutte contre la fraude fiscale ou sociale, ou des traitements de détection de risques psycho-sociaux chez des enfants, etc. ;

— d'algorithmes auto-apprenant de type « *machine learning* », au paramétrage dynamique, susceptibles d'évoluer dans le temps.

Or, en l'état, le projet de loi ne permet pas d'accroître les garanties applicables en fonction des catégories de traitements algorithmiques mis en œuvre, alors même que ces traitements sont susceptibles de faire peser des risques très variables sur les droits et libertés des personnes.

Le Gouvernement estime pour sa part que l'obligation d'information, issue de l'article L. 311-3-1 du code des relations du public et de l'administration, ne constitue pas simplement une règle de transparence, mais aussi, d'une part, une information proactive de l'usager et, de l'autre, par voie de conséquence directe, une maîtrise sur les règles qui doivent pouvoir être communiquées loyalement à la personne concernée, y compris en cas d'actualisations. Elle est complétée par l'article 39 de la loi n° 78-17 et le règlement qui prévoient également une information de la personne concernée. Il estime par ailleurs que le droit au recours hiérarchique ou gracieux de droit commun implique une garantie d'intervention humaine *a posteriori*.

L'enjeu principal, en définitive, ne serait pas celui d'une intervention humaine entre la décision algorithmique et sa notification mais :

— d'une intervention humaine *ab initio*, dans l'édiction des règles et dans leur mise en œuvre par l'algorithme : c'est le sens de l'obligation de maîtrise de

l'algorithme insérée dans l'article du projet de loi (et qui était déjà affirmée par l'article 16 de la loi pour une République numérique) ;

— et d'une intervention humaine *a posteriori* pour réformer des décisions dans certaines situations particulières qui seront portées le cas échéant à la connaissance de l'administration.

3. La position de la Commission

Sur proposition de votre rapporteure, la **Commission a clarifié, à l'article 14, le principe selon lequel aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données** ainsi que les **exceptions à ce principe et les garanties minimales applicables dans ces cas-là.**

S'agissant des exceptions mentionnées au *a* et *c* du *2* de l'article 22 du règlement général sur les données personnelles autorisant la prise d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, lorsqu'elle résulte de **la conclusion ou de l'exécution d'un contrat** entre la personne concernée et un responsable du traitement ou lorsqu'elle est fondée **sur le consentement explicite de la personne concernée**, la Commission a notamment précisé la nécessité de respecter les **garanties minimales posées par le *3* de l'article 22 précité**, à savoir :

– le droit de la personne concernée d'obtenir une **intervention humaine** de la part du responsable du traitement ;

– le droit d'**exprimer son point de vue** ;

– le droit de **contester la décision**.

S'agissant des décisions administratives individuelles exclusivement fondées sur un traitement automatisé de données, la Commission, faisant usage de la marge de manœuvre offerte par le *b* du même article 22 du règlement précité, a précisé que la **maîtrise du traitement algorithmique et de ses évolutions** par le responsable de traitement, doit permettre d'**expliquer, en détails et sous une forme intelligible, à la personne concernée, la manière dont le traitement a été mis en œuvre à son égard**. Sont donc explicitement interdites les décisions administratives individuelles à partir d'un traitement fondé sur un algorithme auto-apprenant (algorithme « boite noire »).

*

* *

La Commission examine l'amendement CL235 de la rapporteure.

Mme la rapporteure. Cet amendement vise à clarifier les exceptions au droit de s'opposer au profilage et les garanties minimales applicables dans ces cas.

La Commission ***adopte*** *l'amendement.*

Puis elle ***adopte*** *l'amendement de précision CL237 de la rapporteure.*

Elle ***adopte*** *ensuite l'article 14* ***modifié.***

Article 15
(III [nouveau] de l'art. 40 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Limitation du droit à la communication d'une violation de données

Dispositions européennes :

L'article 23 du règlement (UE) 2016/679103 prévoit une marge de manœuvre importante qui permet aux États membres de limiter l'ensemble des droits définis aux articles 12 à 22 du règlement, à savoir, outre les droits déjà prévus par la loi n° 78-17, le droit à l'effacement (article 17 du règlement) et le droit à la portabilité des données (article 20), ainsi que le droit à la communication d'une violation de données régi par l'article 34, *« lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir* » certaines finalités, missions ou objectifs listés.

Résumé du dispositif national et effets principaux :

Le présent article complète les dérogations prévues par la loi n° 78-17 en prévoyant qu'un décret en Conseil d'État, pris après avis de la CNIL, fixe la liste des traitements et des catégories de traitements autorisés à déroger au droit à la communication d'une violation de données, pour les cas dans lesquels la communication d'une divulgation ou d'un accès non autorisé à ces données est susceptible de présenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique, et lorsque sont en cause des traitements ou catégories de traitements nécessaires au respect d'une obligation légale ou à l'exercice d'une mission d'intérêt public.

L'effet concret de cette disposition est de permettre aux responsables de traitement de ne pas prévenir la personne dont les données ont fait l'objet d'une violation par un tiers dans des conditions mettant en cause, à raison de données ou à raison de l'emploi de la personne (par exemple s'il s'agit d'un agent des forces de sécurité ou d'un militaire), la sécurité ou la défense, afin de mieux assurer la lutte contre les auteurs de ces violations.

Modifications adoptées par la commission des Lois :

La Commission a adopté cet article sous réserve de modifications rédactionnelles.

1. L'état du droit

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés consacre la section 2 du chapitre V aux droits des personnes à l'égard des traitements de données à caractère personnel.

Elle ne prévoit pas de restriction générale aux droits prévus pour la protection des données à caractère personnel.

Des limitations à certains droits sont en revanche prévues à :

— l'article 38 : limitation au droit d'opposition « *lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement* » ;

— l'article 39 en matière de droit d'accès, le responsable de traitement pouvant « *s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique* ». Le droit d'accès ne s'applique pas non plus « *lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique* » ;

— l'article 40 qui prévoit que le droit de rectification et le droit à l'effacement ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire pour exercer le droit à la liberté d'expression et d'information, pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit à l'effacement est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement, et enfin à la constatation, à l'exercice ou à la défense de droits en justice.

Ces restrictions sont reprises, précisées ou complétées dans les textes autorisant la création de traitements de données. Par exemple, l'article L. 4123-9-1 du code de la défense prévoit, s'agissant des traitements dont la finalité est fondée sur la qualité de militaires des personnes qui y figurent, que les personnes concernées ne sont averties, en cas de divulgation ou d'accès non autorisé à leurs données, qu'après l'accord du ministère compétent.

2. Le dispositif proposé

a. Le règlement général sur la protection des données

L'article 23 du règlement (UE) 2016/679 offre la possibilité pour les États membres de déroger à la plupart des droits garantis au profit des destinataires d'un traitement, mentionnés aux articles 12 à 22 et 34 du règlement, pour des motifs d'intérêt général largement définis, à condition d'entourer cette dérogation des garanties nécessaires à la préservation des droits et libertés fondamentales. Les droits visés sont l'ensemble des droits définis à la section 1 du chapitre III du règlement, à savoir, outre les droits déjà prévus par la loi n° 78-17, le droit à l'effacement (article 17 du règlement), le droit à la portabilité des données (article 20) et le droit à la communication d'une violation de données à caractère personnel (article 34).

Le considérant 73 du règlement précise que : « *Des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données, au droit à la portabilité des données, au droit d'opposition, aux décisions fondées sur le profilage, ainsi qu'à la communication d'une violation de données à caractère personnel à une personne concernée et à certaines obligations connexes des responsables du traitement peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ou de manquements à la déontologie des professions réglementées, et pour garantir d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés pour des motifs d'intérêt public général, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires. Il y a lieu que ces limitations respectent les exigences énoncées par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.* »

b. Le projet de loi

Le présent article, en complétant l'article 40 de la loi n° 78-17 par un III, prévoit la possibilité d'une limitation à être informé des violations d'un traitement de données personnelles, régi par l'article 34 du règlement, pour les seuls

traitements répondant à une obligation légale, et aux seules fins de protection de la sécurité nationale, de la défense nationale ou de la sécurité publique.

Il s'agit de permettre aux responsables de traitement de ne pas prévenir la personne dont les données ont fait l'objet d'une violation par un tiers dans des conditions mettant en cause, à raison de données ou à raison de l'emploi de la personne (par exemple s'il s'agit d'un agent des forces de sécurité ou d'un militaire), la sécurité ou la défense, afin de mieux assurer la lutte contre les auteurs de ces violations.

Sont notamment visés par ces dispositions les traitements comportant des données personnelles à caractère sensible relatives, en particulier, à la qualité de militaire (article 117 de la loi n° 2016-731 du 3 juin 2016) ou à des agents du ministère de la défense occupant des fonctions sensibles (traitements de données de ressources humaines ou du service de santé des armées).

Le présent article prévoit qu'un décret en Conseil d'État, pris après avis de la CNIL, fixe la liste des traitements et des catégories de traitement autorisés à déroger au droit à la communication d'une violation de donnée.

Dans son avis, le Conseil d'État a estimé que cette limitation nouvelle était justifiée et suffisamment précise pour permettre un contrôle de l'adéquation de la restriction aux finalités poursuivies [(1)].

*

* *

La Commission ***adopte*** *l'amendement rédactionnel CL210 de la rapporteure.*

Puis elle ***adopte*** *l'article 15* ***modifié.***

CHAPITRE VI
Voies de recours

Article 16 A (nouveau)
(art. 43 *ter* de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Action de groupe en réparation des préjudices matériels et moraux

Résumé du dispositif et effets principaux :

Cet article étend la possibilité pour les associations agréées d'exercer une action de groupe, avec ou sans mandat, afin d'obtenir la réparation des préjudices matériels et moraux subis par les personnes concernées par la violation de leurs données personnels par un responsable de traitement ou son sous-traitant.

(1) Voir l'avis sur le site : http://www.assemblee-nationale.fr/15/pdf/projets/pl0490-ace.pdf.

Dispositions européennes concernées :

Les articles 80 et 82 du règlement général sur la protection des données et les articles 55 et 56 de la directive relative aux traitements en matière pénale permettent aux États membres de prévoir la possibilité pour un organisme, une organisation ou une association d'introduire, avec ou sans mandat, une action de groupe en réclamation afin d'obtenir réparation des préjudices causés à une personne concernée si elle considère que les droits de cette personne prévus dans le règlement ont été violés du fait d'un traitement de données.

Dernières modifications législatives intervenues :

La loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e^ siècle a introduit une nouvelle modalité de recours juridictionnel en créant une action de groupe en matière de protection des données à caractère personnel ouverte devant le juge judiciaire et le juge administratif. Cette action de groupe, avec ou sans mandat, permet de solliciter du juge la cessation d'un manquement par un responsable de traitement (article 43 *ter* de la loi n° 78-17) mais ne permet pas, en revanche, d'exercer une telle action pour obtenir réparation du dommage ainsi causé.

1. Le droit en vigueur

L'action de groupe est une procédure qui permet à un même demandeur de représenter les intérêts en justice d'un groupe indéterminé d'individus lésés par le comportement d'une même personne.

Introduite en droit français par l'article 1^er^ de la « loi Hamon » du 17 mars 2014, l'action de groupe était à l'origine seulement applicable dans les domaines de la consommation et de la concurrence, puis fut étendue au domaine de la santé par l'article 184 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (dite « Loi Touraine »).

Si ces deux procédures présentaient un grand nombre de similarités, il a été décidé, afin de prévenir le risque de multiplication de procédures d'action de groupe aux règles très différentes, de créer, dans la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e^ siècle, un cadre commun aux actions de groupe et d'ouvrir la voie à des actions de groupe dans les domaines de la lutte contre les discriminations, la protection de l'environnement et la protection des données à caractère personnel.

L'article 91 de la loi nouvelle du 18 novembre 2016 a introduit ainsi un article 43 *ter* à la loi Informatique et libertés n° 78-17 du 6 janvier 1978 selon lequel : « *Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe peut*

être exercée devant la juridiction civile ou la juridiction administrative compétente ».

Au titre du IV de l'article 43 *ter*, peuvent seules exercer cette action :

— les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ;

— les associations de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 811-1 du code de la consommation, lorsque le traitement de données à caractère personnel affecte des consommateurs ;

— les organisations syndicales de salariés ou de fonctionnaires représentatives au sens des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail ou du III de l'article 8 *bis* de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ou les syndicats représentatifs de magistrats de l'ordre judiciaire, lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre.

Il faut toutefois relever une particularité de l'action de groupe dans le domaine de la protection des données personnelles par rapport à celle applicable dans tous les autres domaines prévus par la loi du 18 décembre 2016 : cette action de groupe tend exclusivement à la cessation des manquements à la loi de 1978, et non à la réparation des préjudices subis. Par conséquent, le juge, s'il constate l'existence d'un manquement, ne peut qu'enjoindre au défendeur de cesser ou de faire cesser ledit manquement et de prendre, dans un délai qu'il fixe, toutes les mesures utiles à cette fin, au besoin avec l'aide d'un tiers qu'il désigne. Lorsque le juge prononce une astreinte, celle-ci est liquidée au profit du Trésor public.

À l'inverse, dans les domaines de la consommation et de la concurrence, l'action de groupe peut tendre à la réparation des « petits préjudices » tandis que dans les domaines de la lutte contre les discriminations, de la santé et de la protection de l'environnement, la loi du 18 décembre 2016 a finalement opté pour autoriser, en cas de constatation d'un manquement, la possibilité d'exercer, par voie de mandat, une action de groupe visant à la réparation des préjudices subis (articles 85 à 90 de la loi).

2. Les dispositions européennes

L'article 58.5 du règlement (UE) 2016/679 dispose que : « *Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement* ».

Le chapitre VIII du règlement relatif aux voies de recours, à la responsabilité et aux sanctions prévoit notamment un droit à réparation et responsabilité au bénéfice de la personne concernée par une violation de ses données personnelles (article 82).

Relèvent en outre des marges de manœuvre des États membres la possibilité d'autoriser une personne concernée à donner mandat à un organisme, une organisation ou une association afin d'exercer une action de groupe en vue d'obtenir réparation des préjudices subis en cas de manquement (article 80.1) ou d'exercer cette action, indépendamment de tout mandat confié par une personne concernée (article 80.2).

La directive relative aux traitements en matière pénale prévoit des dispositions très proches du règlement en autorisant la représentation par la voie d'un mandat (article 55) pour mettre en œuvre le droit à réparation prévu à l'article 56.

3. Le dispositif proposé par le projet de loi

Contrairement au choix du Gouvernement britannique par exemple, le projet de loi ne modifie pas le droit en vigueur applicable à l'action de groupe dans le domaine des données personnelles et n'étend donc pas l'action de groupe avec mandat aux fins de réparation des préjudices subis liés à la constatation d'un manquement à la loi informatique et liberté.

Dans l'étude d'impact, le Gouvernement fait valoir le « caractère récent » de l'article 43 *ter* introduit par la loi du 18 décembre 2016 et « *l'opposition du législateur national d'étendre l'action de groupe aux demandes en réparation* » au regard des débats parlementaires de l'époque.

Dans son avis sur l'article 16, la CNIL, comme de nombreuses associations auditionnées par votre rapporteure, a regretté ce choix.

4. La position de la Commission

Sur proposition de votre rapporteure, la Commission a fait le choix d'utiliser la marge de manœuvre laissée par l'article 80 du règlement général sur la protection des données pour **étendre l'action de groupe** en constatation d'un manquement du responsable de traitement ou de son sous-traitant, introduite par la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, **à la possibilité d'engager une action de groupe, avec ou sans mandat, destinée à obtenir réparation des préjudices matériels et moraux subis par la personne concernée, lorsqu'elle considère que ses droits ont été violés du fait du traitement** (**alinéa 1er de l'article 16 A**).

Cette action de groupe s'exerce **dans le cadre de la procédure individuelle de réparation définie par la loi « Justice du XXIe siècle »** précitée.

Cette procédure comprend trois phases :

– le juge statue sur la responsabilité du défendeur ;

– il définit le groupe de personnes susceptibles de bénéficier de l'action de groupe (critères de rattachement au groupe et préjudices susceptibles d'être indemnisés) ;

– il fixe les délais dans lesquels les éventuelles victimes peuvent adhérer au groupe pour se prévaloir du jugement sur la responsabilité. Pour cette dernière phase, des mesures de publicité sont prévues.

La procédure individuelle de réparation des préjudices permet aux victimes d'un manquement en matière de données personnelles d'adhérer au groupe défini par le juge en demandant réparation au défendeur ou au requérant, ce dernier recevant mandat aux fins d'indemnisation. Le défendeur déclaré responsable devra indemniser chaque victime remplissant les critères de rattachement au groupe et ayant adhéré à celui-ci.

L'extension de l'action de groupe à l'action en réparation est justifiée pour au moins **deux raisons**. D'une part, l'action de groupe en matière de données personnelles était la **seule action de groupe prévue en droit français pour laquelle l'action en réparation n'était pas ouverte** ; d'autre part, l'action en réparation des dommages matériels et moraux permettra de **rendre l'action de groupe beaucoup plus effective en France**.

Votre rapporteure estime que d'autres mesures en complément pourraient être envisagées pour renforcer davantage l'effectivité de cette nouvelle voie de droit comme la possibilité pour le juge de condamner le responsable de traitement ou son sous-traitant, auteur d'un manquement, à rembourser à l'association ou l'organisation qui en a fait la demande les frais engagés par celle-ci pour exercer cette action de groupe, qui vont au-delà de la simple condamnation aux dépends au sens de l'article 695 du code de procédure civile.

*

* *

La Commission est saisie de l'amendement CL262 de la rapporteure.

Mme la rapporteure. La loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle a élargi aux discriminations, à l'environnement et aux données à caractère personnel le champ des actions de groupe, introduites par la loi du 17 mars 2014 relative à la consommation.

Le présent amendement, décisif, vise à introduire la possibilité d'exercer une action de groupe tendant à la réparation des préjudices subis en raison d'un manquement aux dispositions de la loi du 6 janvier 1978.

L'action de groupe est un outil qui permettra à l'ensemble du texte de s'appliquer, puisque les citoyens disposeront de cette voie de recours pour obtenir réparation des préjudices matériels et moraux subis en cas de violation de leurs données personnelles. Il est en effet très compliqué pour un individu isolé d'ester en justice dans ce domaine, en raison de la technicité du sujet et de la complexité des démarches. Il est nécessaire que des associations puissent soutenir les personnes concernées et défendent leur intérêt.

M. Guillaume Vuilletet. Notre objectif est de convaincre les citoyens qu'ils peuvent être défendus face à une technologie, un monde qui leur paraît parfois très abscons et fort lointain.

M. Rémy Rebeyrotte. Cet amendement constitue un progrès significatif par rapport au texte initial.

Mme Christine Hennion. Cela me semble d'autant plus nécessaire que ce droit existe déjà dans d'autres pays européens. Dans la mesure où un Français peut bénéficier d'une action de groupe intentée dans un autre pays, il serait illogique qu'il ne dispose pas de ce droit en France.

La Commission ***adopte*** *l'amendement. L'article 16* A *est ainsi rédigé.*

Avant l'article 16

La Commission examine l'amendement CL70 de M. Éric Bothorel.

M. Éric Bothorel. Dans sa délibération du 30 novembre 2017 sur le présent projet de loi, la CNIL a explicitement regretté l'absence de droit à réparation et préconisé d'élargir les objectifs de l'actuelle action de groupe en donnant la possibilité aux citoyens de demander réparation de leur préjudice. Tel est l'objet de mon amendement CL70. Néanmoins, je le retire car il est très proche du CL262 tout juste adopté.

L'amendement est ***retiré****.*

Article 16
(art. 43 *quater* [nouveau] de la loi n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés)
Introduction d'une possibilité de mandater des associations pour exercer ses droits aux recours

Dispositions européennes :

L'article 80 du règlement général sur la protection des données impose aux États membres de prévoir un droit pour les personnes concernées de mandater un organisme, une organisation ou une association afin d'introduire une réclamation auprès d'une autorité de contrôle (article 77) ou d'exercer un recours juridictionnel

contre une autorité de contrôle (article 78) ou contre un responsable de traitement ou un sous-traitant (article 79) ou encore d'exercer une action en réparation (article 82).

Résumé du dispositif national et effets principaux :

Le présent article ouvre la possibilité de mandater les associations mentionnées au IV de l'article 43 *ter* de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, pour exercer une réclamation auprès d'une autorité de contrôle (article 77), d'exercer un recours juridictionnel contre une autorité de contrôle (article 78) ou contre un responsable de traitement ou un sous-traitant (article 79) au nom de la personne concernée.

Modifications adoptées par la commission des Lois :

La Commission a adopté cet article sous réserve de modifications rédactionnelles.

1. L'état du droit

Une personne concernée par un traitement de données dispose de deux voies de recours pour faire constater un manquement à la loi Informatique et Libertés entraînant une violation de ses données personnelles :

— elle peut déposer un recours auprès de la Commission nationale de l'informatique et des libertés (CNIL).

L'article 11 2° c) de la loi n° 78-17 prévoit ainsi que la CNIL reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements et informe leurs auteurs des suites données à celles-ci. Ce droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés est désormais consacré à l'article 77 du règlement (UE) 2016/679.

Les décisions de la CNIL au titre de ses missions de contrôle ou de régulation sont susceptibles d'être l'objet d'un recours devant le Conseil d'État statuant en premier et dernier ressort (article R. 311-1 4° du code de justice administrative). L'article 46 de la loi n° 78-17 précise à cet égard que : « *les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'État* ».

— elle peut déposer un recours individuel devant les juridictions compétentes (pénale, civile ou administrative) dans les conditions de droit commun.

2. Le dispositif proposé

- ***Le règlement général sur la protection des données***

L'article 58.5 du règlement (UE) 2016/679 dispose que : « *Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter*

toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement ».

Le chapitre VIII du règlement relatif aux voies de recours, à la responsabilité et aux sanctions impose aux États membres de prévoir, pour la personne concernée :

– le droit d'introduire une réclamation auprès d'une autorité de contrôle (article 77) ;

– le droit à un recours juridictionnel effectif contre une autorité de contrôle (article 78) ;

– le droit à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant (article 79) ;

– la possibilité d'être représentée par la voie d'un mandat (article 80)

– et un droit à réparation et responsabilité (article 82).

D'autres modalités de recours relèvent des marges de manœuvre des États membres telles que la possibilité d'étendre le mandat mentionné précédemment afin d'exercer une action de groupe en vue d'obtenir réparation des préjudices subis en cas de manquement (article 80.1) et la possibilité pour un organisme, une organisation ou une association, d'exercer les droits définis ci-dessus, indépendamment de tout mandat confié par une personne concernée (article 80.2). Cette marge de manœuvre a été mise en œuvre par la Commission des Lois dans le cadre de l'adoption de l'article 16 A (voir *supra*).

- ***La directive relative aux traitements en matière pénale***

Les articles 52 à 56 de la directive relative aux traitements en matière pénale prévoient des dispositions très proches du règlement en vue de garantir aux personnes concernées le droit d'introduire une réclamation auprès d'une autorité de contrôle (article 52), le droit à un recours juridictionnel effectif contre une autorité de contrôle (article 53), le droit à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant (article 54), leur représentation par la voie d'un mandat pour mettre en œuvre les articles 52 à 54 (article 55) et un droit à réparation (article 56).

- ***Le projet de loi***

Le Gouvernement a fait le choix, à l'article 16, d'une transposition *a minima* des dispositions européennes en ouvrant simplement la possibilité pour toute personne concernée de donner mandat aux associations mentionnées au IV de l'article 43 *ter* de la loi Informatique et Libertés, pour leur permettre d'exercer

en son nom un recours en constatation d'un manquement de la part d'un responsable de traitement en vue de faire cesser ce manquement (voir *infra*).

La CNIL a regretté le fait qu'il ne soit pas fait référence dans le dispositif du présent article à l'article 55 de la directive, qui ouvre les mêmes possibilités de recours que le règlement, ce qui ne permettrait pas d'assurer une bonne transposition [(1)].

Toutefois, sur ce point, le Conseil d'État a considéré que, dans l'hypothèse où les dispositions de la directive sont strictement ou quasiment identiques à celles du règlement, « *des renvois précis à certaines dispositions du règlement peuvent valablement suffire à transposer des articles de la directive, notamment ceux relatifs aux définitions, à la responsabilité du sous-traitant, aux obligations de sécurité, à la coopération avec la CNIL et à la notification des violations des données personnelles. Ainsi, il est fait renvoi, au sein du nouveau chapitre XIII de la loi du 6 janvier 1978, à des articles ou subdivisions d'articles du règlement pour transposer les dispositions similaires de la directive*. » [(2)].

*

* *

La Commission ***adopte*** *successivement les amendements rédactionnels CL211 et CL218 de la rapporteure.*

Elle ***adopte*** *ensuite l'article 16* ***modifié****.*

Article 17

(art. 43 *quinquies* [nouveau] de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Nouvelle voie de recours en cas de transferts internationaux de données

Dispositions européennes :

Les articles 44 à 50 du règlement général sur les données personnelles et les articles 35 à 40 de la directive sur le traitement des données en matière pénale régissent les transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, en particulier les transferts fondés sur une décision d'adéquation de la Commission européenne.

De plus, un arrêt de la Cour de Justice de l'Union européenne (CJUE) du 6 octobre 2015 (C-362/14), *Maximillian Schrems*, impose au législateur national de prévoir une voie de droit spécifique permettant à l'autorité de contrôle de l'utilisation des données personnelles de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité d'une décision

(1) Voir l'avis sur le site : https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf.

(2) Voir l'avis sur le site : http://www.assemblee-nationale.fr/15/pdf/projets/pl0490-ace.pdf.

d'adéquation de la Commission européenne, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision devant la Cour de Justice de l'Union européenne.

Résumé du dispositif et effets principaux :

Le nouvel article 43 *quinquies* de la loi n° 78-17 permet à la Commission nationale Informatique et Liberté (CNIL) d'ester pour obtenir la saisine de la Cour de Justice de l'Union européenne (CJUE) 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 ainsi que la CNIL peut demander au Conseil d'État 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 CJUE 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. Si le Conseil d'État partage les doutes de la CNIL sur la validité de cet acte, il devra poser une question préjudicielle à la Cour de justice de l'Union européenne en application de l'article 267 du Traité sur le fonctionnement de l'Union européenne.

Modifications adoptées par la commission des Lois :

À l'initiative de votre rapporteure, la Commission a supprimé la possibilité pour le Conseil d'État d'ordonner, sur demande de la CNIL, la « *cessation* » du transfert de données à caractère personnel vers un État tiers pour ne conserver que la possibilité d'ordonner sa « *suspension* », dans la mesure où la décision du Conseil d'État est nécessairement temporaire.

1. La jurisprudence de la Cour de Justice de l'Union européenne

a. Le litige initial

La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu que si le pays en question assure un niveau de protection adéquat à ces données. La Commission peut constater qu'un pays tiers assure, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection adéquat. Enfin, chaque État membre doit désigner une ou plusieurs autorités publiques chargées de surveiller l'application, sur son territoire, des dispositions nationales adoptées sur le fondement de la directive (« autorités nationales de contrôle »).

En l'espèce, M. Maximillian Schrems, un citoyen autrichien, utilisait Facebook depuis 2008. Comme pour les autres abonnés résidant dans l'Union, les

données fournies par M. Schrems à Facebook étaient transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles faisaient l'objet d'un traitement. M. Schrems a déposé une plainte auprès de l'autorité irlandaise de contrôle, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-Unis (en particulier la National Security Agency ou « NSA »), le droit et les pratiques des États-Unis n'offraient pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays. L'autorité irlandaise a rejeté la plainte, au motif notamment que, dans sa décision du 26 juillet 2002, la Commission européenne a considéré que, dans le cadre du régime dit de la « sphère de sécurité » (ou « Safe-Harbor »), les États-Unis assuraient un niveau adéquat de protection aux données à caractère personnel transférées. Ce régime de la « sphère de sécurité » comprend une série de principes relatifs à la protection des données à caractère personnel auxquels les entreprises américaines peuvent souscrire volontairement.

Saisie de l'affaire, la High Court of Ireland (Haute Cour de justice irlandaise) souhaitait savoir si cette décision de la Commission avait pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat et, le cas échéant, de suspendre le transfert de données contesté. Elle a donc posé une question préjudicielle à la Cour de Justice de l'Union européenne.

b. La solution retenue par la CJUE

Dans son arrêt du 6 octobre 2015, la CJUE a estimé que l'existence d'une décision de la Commission constatant qu'un pays tiers assure un niveau de protection adéquat aux données à caractère personnel transférées ne saurait annihiler ni même réduire les pouvoirs dont disposent les autorités nationales de contrôle en vertu de la Charte des droits fondamentaux de l'Union européenne et de la directive.

La Cour a considéré tout d'abord qu'aucune disposition de la directive n'empêche les autorités nationales de contrôler les transferts de données personnelles vers des pays tiers ayant fait l'objet d'une décision de la Commission. Ainsi, même en présence d'une décision de la Commission, les autorités nationales de contrôle, saisies d'une demande, doivent pouvoir examiner en toute indépendance si le transfert des données d'une personne vers un pays tiers respecte les exigences posées par la directive.

Néanmoins, la Cour a rappelé qu'elle était seule compétente pour constater l'invalidité d'un acte de l'Union, tel qu'une décision de la Commission. Par conséquent, lorsqu'une autorité nationale ou bien la personne ayant saisi l'autorité nationale estime qu'une décision de la Commission est invalide, cette autorité ou cette personne doit pouvoir saisir les juridictions nationales pour que, dans le cas où elles douteraient elles aussi de la validité de la décision de la Commission, elles puissent renvoyer l'affaire devant la Cour de justice. C'est donc en dernier lieu à

la Cour que revient la tâche de décider si une décision de la Commission est valide ou non.

La Cour a vérifié, dans cette affaire, la validité de la décision de la Commission du 26 juillet 2000. Elle a considéré que la Commission était tenue de constater que les États-Unis assurent effectivement, en raison de leur législation interne ou de leurs engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte. Or, la Cour relève que la Commission n'a pas opéré un tel constat, mais qu'elle s'est bornée à examiner le régime de la sphère de sécurité.

Sans qu'il y ait besoin, pour la Cour, de vérifier si ce régime assure un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union, la Cour a relevé que celui-ci est uniquement applicable aux entreprises américaines qui y souscrivent, sans que les autorités publiques des États-Unis y soient elles-mêmes soumises. En outre, les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis l'emportent sur le régime de la sphère de sécurité, si bien que les entreprises américaines sont tenues d'écarter, sans limitation, les règles de protection prévues par ce régime lorsqu'elles entrent en conflit avec de telles exigences. Le régime américain de la sphère de sécurité rendait ainsi possible des ingérences, par les autorités publiques américaines, dans les droits fondamentaux des personnes, la décision de la Commission ne faisant état ni de l'existence, aux États-Unis, de règles destinées à limiter ces éventuelles ingérences ni de l'existence d'une protection juridique efficace contre ces ingérences.

La Cour a considéré que cette analyse du régime était corroborée par deux communications de la Commission, d'où il ressort notamment que les autorités des États-Unis peuvent accéder aux données à caractère personnel transférées à partir des États membres vers ce pays et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert et au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale. De même, la Commission a constaté qu'il n'existait pas, pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression.

S'agissant du niveau de protection substantiellement équivalent avec les libertés et droits fondamentaux garantis au sein de l'Union, la Cour a constaté que, en droit de l'Union, une règlementation n'est pas limitée au strict nécessaire, dès lors qu'elle autorise de manière généralisée la conservation de toutes les données à caractère personnel de toutes les personnes dont les données sont transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception ne soient opérées en fonction de l'objectif poursuivi et sans que des critères objectifs ne soient prévus en vue de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure. La Cour a ajouté qu'une

règlementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée.

De même, la Cour a relevé qu'une règlementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, portait atteinte au contenu essentiel du droit fondamental à une protection juridictionnelle effective, une telle possibilité étant inhérente à l'existence d'un État de droit.

Enfin, la Cour a constaté que la décision de la Commission du 26 juillet 2000 privait les autorités nationales de contrôle de leurs pouvoirs, dans le cas où une personne remet en cause la compatibilité de la décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes. La Cour a donc jugé que la Commission n'avait pas la compétence de restreindre ainsi les pouvoirs des autorités nationales de contrôle.

Pour toutes ces raisons, la Cour a déclaré la décision de la Commission du 26 juillet 2000 invalide. Cet arrêt a pour conséquence que l'autorité irlandaise de contrôle était tenue d'examiner la plainte de M. Schrems avec toute la diligence requise et qu'il lui appartenait, au terme de son enquête, de décider s'il convenait, en vertu de la directive, de suspendre le transfert des données des abonnés européens de Facebook vers les États-Unis au motif que ce pays n'offrait pas un niveau de protection adéquat des données personnelles.

2. Le droit en vigueur

La directive 95/46/CE, objet du litige initial, est abrogée par le règlement (UE) 2016/679 relatif à la protection générale des données personnelles qui instaure de nouvelles règles relatives aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales.

Néanmoins, le droit actuel ne prévoit pas la voie de recours définie dans l'arrêt *Maximillian Schrems* du 6 octobre 2015 précité, à savoir la possibilité pour la Commission nationale de l'informatique et des libertés de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision d'adéquation de la Commission européenne, à un renvoi préjudiciel aux fins de l'appréciation de la validité de cette décision par la Cour de justice de l'Union européenne.

Une absence de mesure législative exposerait la France à une procédure en manquement, en application des articles 258 à 260 du Traité sur le fonctionnement de l'Union européenne, dès lors qu'il s'agirait d'une méconnaissance d'une obligation découlant d'un texte européen.

3. Le dispositif proposé

L'article 17 du projet de loi introduit un nouvel article 43 *quinquies* au sein de la section 2 du chapitre V de la loi Informatique et Liberté qui transpose l'exigence posée par la CJUE dans le cadre de l'arrêt Maximillian Schrems du 6 octobre 2015 de la manière présentée ci-après.

Lorsqu'elle sera saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale de l'informatique et des libertés (CNIL) pourra demander au Conseil d'État d'ordonner, dans l'attente de l'appréciation par la CJUE – qu'il aura saisi à titre préjudiciel s'il partage des doutes de la CNIL – de la validité d'une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679, la suspension ou la cessation du transfert de données en cause, le cas échéant sous astreinte. La CNIL devra alors assortir ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de tels actes adoptés par la Commission européenne. Dans son avis sur le présent projet de loi, le Conseil d'État considère que la demande de question préjudicielle doit être posée, à peine d'irrecevabilité de la demande de suspension provisoire du transfert.

Afin de donner un plein effet utile à cette voie de recours, et dans un souci de cohérence et de protection accrue des données à caractère personnel, il a été fait le choix d'élargir cette voie de recours à l'ensemble des actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 du règlement (UE) 2016/679, et pas uniquement les décisions d'adéquation, conformément à l'avis de la CNIL sur le présent article : clause-type de protection des données, code de conduite, mécanisme de certification.

Cette nouvelle voie de droit est également étendue à l'égard des décisions d'adéquation de la Commission européenne prises sur le fondement de l'article 36 de la directive (UE) 2016/680, lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle.

Le choix du Conseil d'État pour connaître de cette nouvelle voie de recours, par dérogation à la compétence de premier ressort des tribunaux administratifs, a été fait en considération d'une bonne administration de la justice. Actuellement, le Conseil d'État est compétent pour connaître, en premier et dernier ressort, des décisions prises par la CNIL au titre de sa mission de contrôle. La décision prise par la CNIL, après que la CJUE se sera prononcée sur la question préjudicielle dont elle aura été saisie, relèvera de la compétence du Conseil d'État en vertu de l'article R. 311-1 du code de justice administrative. En outre, ce nouveau recours, qui porte sur une question sensible relative à la protection des données à caractère personnel transférées vers un pays tiers, suppose qu'il soit statué rapidement.

4. La position de la Commission

Sur proposition de votre rapporteure, la Commission a adopté deux amendements rédactionnels et **supprimé la possibilité pour le Conseil d'État d'ordonner, sur demande de la CNIL, la « cessation » du transfert de données à caractère personnel vers un État tiers**, pour se cantonner à la possibilité d'ordonner "la suspension" du transfert dans la mesure où la décision du Conseil d'État est nécessairement temporaire.

En effet, cette décision ne peut intervenir que dans l'attente de la décision de la CJUE, saisie à titre préjudiciel par le Conseil d'État sur demande de la CNIL, lorsque cette dernière estime fondée la demande d'une personne relative à la protection de ses droits et libertés à l'égard d'un traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers un pays tiers, quand cette personne fait valoir que le droit et les pratiques en vigueur dans celui−ci n'assurent pas un niveau de protection adéquat, malgré une décision d'adéquation de la Commission européenne.

Cette précision est conforme à la décision de la CJUE dans l'arrêt « Schrems » dans laquelle la Cour ne vise que la "suspension" des flux de données.

*

* *

*La Commission **adopte** successivement l'amendement rédactionnel CL212, l'amendement de précision CL229 et l'amendement rédactionnel CL219.*

*Puis elle **adopte** l'article 17 **modifié**.*

Après l'article 17

La Commission examine l'amendement CL69 de M. Éric Bothorel.

M. Éric Bothorel. Conformément à l'esprit qui anime le Règlement général sur la protection des données (RGPD), cet amendement vise à ce que, lorsque l'on commence à utiliser son *smartphone*, sa tablette ou son ordinateur personnel, on ne choisisse pas seulement des paramètres tels que le fuseau horaire ou autres, mais aussi son moteur de recherche, c'est-à-dire son mode d'accès à internet. On pourra ainsi sélectionner, parmi les logiciels disponibles, celui qui servira à naviguer sur internet et à faire des recherches.

Cet amendement ne revient pas à édicter une interdiction, mais au contraire à faire prévaloir la liberté, puisqu'il renforce le consentement et la bonne information des utilisateurs. Ils pourront comparer les performances des logiciels, ce qu'ils offrent, notamment en matière de protection et d'utilisation des données, et même le mode de fonctionnement de l'algorithme. L'utilisateur est aujourd'hui

confronté à des outils pré-installés et il se voit plus ou moins imposer son choix : grâce à cet amendement, il aura une liberté plus grande.

On pourra certes choisir les outils les plus connus, si on le souhaite, mais les différents acteurs entreront dans une saine compétition. Comme ils seront tous entièrement conformes au RGPD, je n'en doute pas, d'autres éléments seront peut-être mis en avant afin d'inciter l'utilisateur.

Mme la rapporteure. J'adhère au principe et à la logique de l'amendement. Néanmoins, tel qu'il est rédigé, il ne me paraît pas avoir sa place dans ce texte, mais plutôt dans le cadre des futures discussions sur l'*ePrivacy* au niveau européen. Nous pourrions toutefois essayer de rattacher ce que vous proposez à la notion de consentement libre : pour qu'il existe, il faut avoir des alternatives. Je vous propose d'y travailler d'ici à la séance, mais je suis désireuse de connaître l'avis de la garde des Sceaux au préalable.

Mme la garde des Sceaux. Je partage votre avis : c'est une vraie question, qui mérite d'être traitée, et j'accepte volontiers que l'on retravaille la rédaction de l'article.

Mme Christine Hennion. Je voudrais par ailleurs souligner que cela reviendrait à appliquer le principe de *privacy by default.*

M. Éric Bothorel. On peut discuter de l'endroit où insérer l'amendement, mais je pense que ce projet de loi est le bon vecteur pour avoir un débat. Une de ses principales vertus sera peut-être d'influer sur la réflexion au niveau européen – elle ne doit pas être uniquement française. J'accepte volontiers la proposition de travailler à une autre rédaction de l'amendement : je le retire donc pour en déposer une version 2.0 en séance. *(Sourires).*

Mme Constance Le Grip. J'adhère, moi aussi, à l'esprit qui est celui de l'amendement. Je conçois que l'on puisse s'interroger sur l'articulation avec le projet de loi, mais il serait préjudiciable d'attendre un texte européen sur l'*ePrivacy*, car les discussions sont loin d'être finies à ce niveau. Nous devons faire passer nos messages dès maintenant. J'apporte mon soutien à l'amendement : quitte à le réécrire un peu, il est important de l'insérer dans le texte.

L'amendement est ***retiré****.*

TITRE III
DISPOSITIONS PORTANT TRANSPOSITION DE LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIVE À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES AUTORITÉS COMPÉTENTES À DES FINS DE PRÉVENTION ET DE DÉTECTION DES INFRACTIONS PÉNALES, D'ENQUÊTES ET DE POURSUITES EN LA MATIÈRE OU D'EXÉCUTION DE SANCTIONS PÉNALES, ET À LA LIBRE CIRCULATION DE CES DONNÉES

La directive 2016/680 du 27 avril 2016 [(1)] constitue le second volet de l'avancée majeure que représente le « paquet européen de protection des données ».

Sur la forme, son **champ d'application** est **vaste**. À la différence de la décision-cadre de 2008 [(2)] qu'elle remplace et qui ne visait que les échanges de données personnelles dans le cadre de la coopération en matière pénale, la directive s'applique à tous les traitements de données pénales mis en œuvre par les autorités compétentes aux fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière et d'exécution de sanctions pénales, y compris la protection contre les menaces à la sécurité publique et la prévention de telles menaces. Seront par exemple concernés le fichier national transfrontière, le fichier STADE, le fichier national des empreintes génétiques (FNAEG), le fichier national des interdits de stade ou le système européen de traitement des données d'enregistrement et de réservation (SETRADER).

Les traitements de données pénales mis en œuvre par toute personne à d'autres fins que celles-ci relèveront du règlement général sur la protection des données [(3)]. Les traitements aux finalités mixtes, relevant à la fois de la directive et du règlement, devront être prévus par un acte législatif ou réglementaire ou un acte répondant aux exigences de clarté, de précision et de prévisibilité. Enfin, les traitements mis en œuvre dans le cadre d'une activité qui se situe hors du champ du droit de l'Union européenne, en particulier ceux de renseignement, continueront de relever de la compétence du droit national.

Sur le fond, la directive a pour effet de **soumettre les fichiers de police et de justice relevant de son champ à un grand nombre des principes généraux et des droits applicables aux personnes concernées tels qu'ils sont prévus par le règlement général sur la protection des données**, sous réserve des

---

(1) Directive (UE) 2016/680 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.

(2) Décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

(3) Voir supra*, le commentaire de l'article 11.*

adaptations et **limitations** justifiées par la nature particulière des traitements en cause et de leurs finalités.

*

* *

Article 18

(art. 32, 41 et 42 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Création d'un droit d'information de la personne et suppression du caractère indirect des droit d'accès, de rectification, d'effacement et de limitation pour les fichiers de police et de justice

Résumé du dispositif et effets principaux :

Le présent article modifie les conditions d'exercice des droits reconnus à la personne concernée par un traitement de données pénales ou intéressant la sûreté de l'État, la défense ou la sécurité publique mis en œuvre par les autorités publiques en vue de les aligner sur celles prévues par la directive 2016/680 du 27 avril 2016 :

– il lève l'exclusion du droit d'information de cette personne dans le cas des traitements ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté et pour ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ;

– il supprime le caractère indirect de l'exercice des droits d'accès, de rectification et d'effacement pour les traitements qui ont pour mission de prévenir, rechercher ou constater des infractions.

Dispositions de la directive concernées : articles 12 à 18.

Dernières modifications législatives intervenues :

Le régime dérogatoire applicable aux droits de la personne concernée face aux « traitements de souveraineté » (défense, sécurité publique, sûreté de l'État, droit pénal) résulte de la transposition, par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, de la directive 95/46/CE du 24 octobre 1995. Cette dernière ne s'appliquant pas à ces catégories de traitements, le législateur a exclu l'application du droit à l'information et a confié à la CNIL le soin de traiter les demandes d'accès à ces traitements.

Modifications adoptées par la commission des Lois :

La Commission a adopté cet article en n'y apportant que des modifications de nature rédactionnelle.

1. L'état du droit

Les fichiers de police et de justice sont aujourd'hui soumis à un droit dérogatoire de la protection des données personnelles, en particulier s'agissant des conditions d'exercice des droits de la personne concernée.

a. L'exercice indirect des droits d'accès, de rectification et d'effacement

Les droits d'accès, de rectification et d'effacement reconnus à la personne par les articles 39 et 40 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés **s'exercent en principe de manière indirecte** :

— pour « *un* ***traitement intéress*****[ant]** ***la sûreté de l'État, la défense ou la sécurité publique*** **» (article 41)** ;

— pour les « *traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de* ***prévenir, rechercher ou constater des infractions****, ou de contrôler ou recouvrer des impositions* » lorsque ces droits sont prévus dans l'acte autorisant la mise en œuvre du traitement (**article 42**).

La demande est adressée à la Commission nationale de l'informatique et des libertés (CNIL) « *qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires* ». Si, en accord avec le responsable du traitement, elle estime que la communication des données ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, elle communique les éléments au requérant. En cas de désaccord, elle informe simplement le requérant qu'elle a procédé aux vérifications nécessaires.

L'acte réglementaire portant création du fichier peut autoriser le responsable du traitement directement saisi à communiquer ces informations « *lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées* ».

b. L'absence de droit à l'information

Par ailleurs, l'**article 32** de la même loi, qui soumet les responsables de traitements à une **obligation d'information** des personnes concernées par les traitements, n'est **pas applicable « *lors d'un traitement* *mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou* ***ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté*** **» (V) ni aux « *traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales*** **» (VI)**.

2. Le dispositif proposé

a. La directive relative aux traitements de données à des fins pénales

La directive 2016/680 du 27 avril 2016 fixe, dans son chapitre III, les règles applicables aux droits des personnes concernées par un traitement de données personnelles mis en œuvre par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière ou d'exécution des sanctions pénales.

i. Le droit à l'information

La directive instaure un **droit à l'information de la personne concernée en matière pénale (article 13)**, en obligeant le responsable du traitement à mettre à sa disposition plusieurs informations :

— un socle minimal d'informations doit lui être communiqué sur demande : identité et coordonnées du responsable, coordonnées du délégué à la protection des données s'il existe, finalités du traitement, droit d'introduire une réclamation auprès de l'autorité de contrôle et coordonnées de cette dernière, droit de demander au responsable l'accès aux données, leur rectification ou leur effacement ainsi que la limitation du traitement ;

— les États peuvent prévoir, dans leur droit national, une liste d'informations à communiquer dans certains cas, dans la mesure où ces informations supplémentaires sont nécessaires au caractère loyal du traitement (base juridique du traitement, durée de conservation des données, destinataires) ;

— les États peuvent, sous réserve de tenir compte des droits fondamentaux de la personne, **« *retarder ou limiter la fourniture des informations à la personne concernée* » ou « *ne pas fournir ces informations* » afin de ne pas gêner des procédures en cours, de ne pas nuire à l'effectivité des finalités poursuivies par le traitement, de protéger la sécurité publique ou nationale ou de protéger les droits et libertés d'autrui**.

ii. Le droit d'accès

La personne concernée a le **droit d'obtenir** du responsable du traitement **la confirmation que des données la concernant sont ou non traitées**, **l'accès à ces données ainsi que certaines informations (article 14)** (1).

Ce droit d'accès peut être restreint, en partie ou totalité (article 15), par décision des États pour les mêmes objectifs et dans les mêmes conditions que le droit à l'information. En cas de limitation de ce droit, le responsable du

(1) Finalités et base juridique du traitement, catégories de données collectées, destinataires de ces données, durée de conservation de celles-ci, existence du droit de demander la rectification ou l'effacement des données ou la limitation du traitement ainsi que du droit de déposer une réclamation auprès de l'autorité de contrôle, communication des données en cours de traitement.

traitement doit en informer la personne concernée « *dans les meilleurs délais* » en précisant les motifs. Cette information n'est pas exigible si elle risque de compromettre l'un des objectifs précédemment cités, auquel cas le responsable informe la personne de son droit d'introduire une réclamation auprès de l'autorité de contrôle ou de former un recours juridictionnel.

iii. Le droit de rectification ou d'effacement des données et à la limitation du traitement

En vertu de l'**article 16**, la personne concernée a le droit d'obtenir du responsable du traitement, « *dans les meilleurs délais* » :

— la **rectification** ou le complément des données inexactes ou incomplètes la concernant ;

— l'**effacement** de certaines données lorsque ne sont pas respectés les principes applicables aux traitements (licéité, sécurité, compatibilité avec les finalités légitimes, conservation, exactitude des données…).

Au lieu d'effacer les données, le responsable peut en limiter le traitement lorsqu'il ne peut être déterminé si les données sont exactes ou non ou lorsqu'elles doivent être conservées à des fins probatoires.

En tout état de cause, la personne est informée par le responsable de tout refus de rectifier ou d'effacer des données ou de limiter le traitement ainsi que des motifs du refus. Ce devoir d'information peut être levé dans les mêmes conditions que pour le droit à l'information et le droit d'accès.

iv. Modalités communes d'exercice de ces droits

Les informations communiquées à la personne concernée dans l'exercice des droits à l'information, d'accès, de rectification, d'effacement et de limitation doivent faire l'objet d'une **transmission claire et gratuite**, sauf en cas de demandes manifestement infondées ou excessives (**article 12**).

La directive pose le **principe d'un exercice direct par la personne concernée de ses droits** auprès du responsable du traitement.

Par exception, **en cas de restriction justifiée par la nécessité de ne pas nuire à la prévention ou à la détection d'infractions pénales et de protéger la sécurité et les intérêts d'autrui, ces droits peuvent s'exercer de manière indirecte**, par l'intermédiaire de l'autorité de contrôle, laquelle doit au moins informer la personne du fait qu'elle a procédé à toutes les vérifications nécessaires et qu'elle conserve la possibilité de former un recours juridictionnel (**article 17**).

Chaque État peut prévoir des modalités particulières d'exercice de ces droits dans le cas de traitements de décisions, dossiers ou casiers judiciaires lors d'une enquête judiciaire et d'une procédure pénale (**article 18**).

b. Le projet de loi

Le présent article vise à mettre le droit français en conformité avec les dispositions de la directive, par coordination avec l'article 19 qui en assure la complète transposition [(1)].

Les I et II lèvent l'exclusion du droit à l'information prévue par les V et VI de l'actuel article 32 de la loi de 1978 **dans le cas des traitements** ayant pour objet **l'exécution de condamnations pénales ou de mesures de sûreté** (I) et **la prévention, la recherche, la constatation ou la poursuite d'infractions pénales** (II), catégories de traitements qui relèvent toutes deux du champ de la directive.

Le **III** ajoute une coordination à l'article 41 de la même loi qui prévoit l'exercice indirect des droits d'accès, de rectification et d'effacement dans le cas de traitements intéressant la sûreté de l'État, la défense ou la sécurité publique. Cette dernière catégorie de traitements étant susceptible, à la différence des deux premières, de relever du champ de la directive, c'est le principe d'un exercice direct de ces droits qui s'appliquera.

Le **IV** a pour effet de **supprimer**, à l'article 42 de cette loi, **le caractère indirect de l'exercice des droits d'accès, de rectification et d'effacement pour les traitements de police judiciaire**.

*

* *

*La Commission **adopte** successivement l'amendement rédactionnel CL151 et l'amendement de précision CL152 de la rapporteure.*

*Puis elle **adopte** l'article 18 **modifié**.*

(1) Voir infra*, le commentaire de l'article 19.*

Article 19
(art. 70-1 à 70-27 [nouveaux] de la loi n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés)
Dispositions applicables aux fichiers de police et de justice

Résumé du dispositif et effets principaux :

Le présent article transpose en droit français les dispositions de la directive 2016/680 du 27 avril 2016 relative aux traitements de données personnelles par la police et les autorités judiciaires en matière pénale.

Il insère un nouveau chapitre au sein de la loi de 1978 dédié à cette catégorie de traitements, qui recense les principes généraux applicables à ces fichiers, les obligations incombant aux autorités et responsables de ces traitements, les droits reconnus aux personnes concernées, assortis des restrictions qui sont susceptibles d'affecter leur portée ou leur exercice, ainsi que les conditions de transfert des données vers des États n'appartenant pas à l'Union européenne.

Dispositions de la directive concernée : articles 1 à 4, 6 à 11, 12 et 13, 15 et 16, 18 à 20, 22 à 25 et 27 à 39.

Dernières modifications législatives intervenues :

Les règles particulières régissant les droits reconnus à la personne concernée par un traitement mis en œuvre afin de prévenir, rechercher ou constater des infractions ou intéressant la sécurité publique résultent de la transposition, par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, de la directive 95/46/CE du 24 octobre 1995.

Modifications adoptées par la commission des Lois :

La Commission a approuvé les orientations retenues par le Gouvernement pour transposer la directive. Outre de nombreuses modifications rédactionnelles, elle a adopté un amendement de Mme Danièle Obono renforçant les conditions applicables à la conservation des données pénales traitées ainsi que deux amendements de votre rapporteure précisant le champ de l'obligation de notification à la personne concernée en cas de restriction de ses droits et les modalités de transmission des informations communiquées à celle-ci par le responsable de traitement.

1. L'état du droit

Les traitements de données à caractère personnel en matière pénale sont pour partie l'objet de règles dérogatoires du droit commun de la législation relative à la protection des données personnelles.

Si les principes généraux de cette législation, les droits reconnus aux personnes concernées ainsi que les obligations incombant aux responsables de

traitements s'appliquent en principe à cette catégorie de traitements, certaines dispositions permettent d'y déroger ou de moduler l'exercice des droits en vue de tenir compte de la nature particulière des fichiers en cause et des finalités poursuivies par ceux-ci. Ainsi, il n'existe **pas de droit à l'information en matière pénale** [(1)] et **les droits de rectification, d'effacement ou de limitation s'exercent de manière indirecte**, par l'intermédiaire de la Commission nationale de l'informatique et des libertés (CNIL) [(2)].

En outre, le droit actuel régit imparfaitement les modalités de transfert de données personnelles en matière pénale vers des États non-membres de l'Union européenne (UE). Il s'agit de la coopération entre autorités judiciaires ou services d'enquête, notamment lorsque la France souhaite obtenir de services de communications électroniques situés à l'étranger des informations utiles à la répression d'infractions commises par internet. Ces transferts peuvent s'effectuer à l'initiative des autorités françaises dans le cadre de commissions rogatoires internationales ou sur demande d'autorités étrangères dans le cadre de conventions d'entraide judiciaire en matière pénale, de conventions d'extradition ou de transfèrement ou d'accords de sécurité intérieure.

Les conditions dans lesquelles de tels transferts sont possibles relèvent du cadre général suivant, applicable aux transferts de données personnelles en dehors de l'Union européenne, fixé par les **articles 68 à 70 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** :

— le transfert de données n'est **possible « *que si cet État assure un niveau de protection suffisant* *de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement* »** : le caractère satisfaisant de cette protection s'apprécie « *en fonction notamment des dispositions en vigueur dans cet État, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées* » (**article 68**) ;

— certaines **dérogations** à l'interdiction de procéder à des transferts en l'absence de garantie suffisante sont toutefois prévues **si la personne a expressément consenti au transfert, si le transfert est nécessaire à la poursuite d'un objectif légitime [(3)], comme la sauvegarde de l'intérêt public**, ou, par décision de la CNIL ou décret en Conseil d'État pris après avis de celle-ci, **si le traitement « *garantit un niveau de protection suffisant* *de la vie privée ainsi que***

---

(1) VI de l'article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Articles 41 et 42 de la même loi.

(3) La sauvegarde de la vie de cette personne (1°) ; la sauvegarde de l'intérêt public (2°) ; le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice (3°) ; la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime (4°) ; l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci (5°) ; la conclusion ou l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers (6°).

des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet » (**article 69**) ;

— des procédures sont prévues pour déterminer le niveau de protection offert par les États tiers, sous la forme d'une coopération entre les États membres de l'Union et la Commission européenne (**article 70**).

Ces dispositions ont été précisées par un décret du 20 octobre 2005 (1) qui a fixé notamment les obligations incombant aux responsables de traitements, par référence à la liste des États, établie par la CNIL, assurant un niveau adéquat de protection au regard de la directive 95/46/CE.

Toutefois, ces dispositions restent d'application difficile pour les transferts internationaux de données pénales. D'une part, la directive de 1995 à laquelle il est fait référence ne s'applique pas dans cette matière. D'autre part, la mise en œuvre de tels transferts ne peut relever que d'une autorisation par décret en Conseil d'État et non de l'exception liée à la sauvegarde de l'intérêt public, aux termes d'un avis du Conseil d'État rendu en 2006 lors de l'examen d'un projet de loi de ratification de l'accord d'entraide judiciaire en matière pénale avec la Chine (2). Or, seule une douzaine d'États a été classée par l'Union européenne ou la CNIL comme ayant un niveau de protection suffisant en matière de protection de la vie privée.

2. Le dispositif proposé

a. La directive

Votre rapporteure décrira plus loin le contenu précis de la directive 2016/680 du 27 avril 2016 en examinant, article par article, la transposition de ses dispositions. Elle se bornera donc ici à en retracer les grands équilibres et les nouveautés qu'elle conduit à introduire dans notre droit national.

En premier lieu, la directive vise à **garantir la protection des données personnelles des personnes impliquées dans une procédure pénale** :

— les données devront être **traitées de manière licite et loyale et pour des finalités déterminées, explicites et légitimes**, en respectant des règles très proches du droit commun de la protection des données personnelles ;

— **les autorités compétentes, les responsables de traitements et, le cas échéant, les sous-traitants sont soumis à certaines obligations**, largement inspirées des règles prévues par le règlement général sur la protection des données, comme celles de mettre à jour les données, de tenir un registre et un journal des activités de traitement, de désigner un délégué à la protection des

(1) Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Voir l'étude d'impact annexée au présent projet de loi, pp. 213-214.

données, d'assurer la sécurité des données ou d'informer l'autorité de contrôle et la personne concernée en cas de violation des données ;

— **les personnes concernées se voient reconnaître des droits, tels que le droit à l'information, le droit d'accès, le droit de rectification ou d'effacement des données et de limitation du traitement** : ces droits s'exerceront par principe **de manière gratuite et directe**, sans le filtre de l'autorité de contrôle, mais pourront faire l'objet de **restrictions** compte tenu des besoins spécifiques des services répressifs et de la diversité des traditions juridiques observées dans cette matière au sein de l'Union européenne.

En second lieu, elle tend à **faciliter l'échange d'informations entre les autorités policières et judiciaires nationales en vue d'améliorer la coopération** dans la lutte contre le terrorisme et les formes graves de criminalité en Europe. À cette fin, elle clarifie le cadre juridique applicable aux transferts de données vers des États n'appartenant pas à l'Union.

Si la loi de 1978, par sa portée générale, comporte déjà certaines des garanties prévues par la directive, d'autres n'existent pas dans notre droit ou ne sont pas identiques dans leur contenu ou leur portée à celles posées par le droit européen.

b. Le projet de loi

Pour les raisons qui précèdent, le présent article transpose dans notre droit les dispositions de la directive en insérant dans la loi de 1978 un **nouveau chapitre XIII spécifique aux traitements pénaux**, comportant les **nouveaux articles 70-1 à 70-27**. À la différence de la solution, complexe et peu lisible, qui aurait consisté à intégrer ces règles à la suite de chaque article de la loi de 1978, ce choix de transposition permet de regrouper, de manière simple et lisible, les dispositions applicables à cette catégorie de traitements.

i. Dispositions générales

- Liste des traitements concernés (article 70-1, alinéas 1 à 3)

La liste des traitements concernés par ces nouvelles règles reprend le champ d'application de la directive. Seront concernés les traitements mis en œuvre **à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite 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 (**1°**), mis en œuvre par « *toute* ***autorité publique compétente*** » ou par « *tout* ***organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique*** » (**2°**).

Ces dispositions sont la transposition de l'article 2 de la directive.

• Licéité des traitements (article 70-1, alinéa 4)

Ces traitements ne seront licites que s'ils sont **nécessaires à l'exécution d'une mission effectuée pour l'une de ces finalités, mis en œuvre par l'une des autorités compétentes** précédemment **mentionnées et respectent les dispositions relatives aux formalités préalables et analyses d'impact**.

Il s'agit de la transposition de l'article 8 de la directive.

• Définition des notions (article 70-1, alinéa 5)

Pour l'application des dispositions relatives à ces traitements, les notions utilisées seront identiques à celles définies au chapitre premier de la loi de 1978. À défaut d'être définies dans ce chapitre, seront applicables les définitions posées par le règlement général sur la protection des données.

Les dispositions de la directive relatives aux définitions étant en grande partie identiques à celles du règlement, un simple renvoi à celui-ci suffit pour la transposer [(1)]. La notion d'« *autorité compétente* », seule notion nécessaire à l'application de la directive à ne pas être définie par le règlement, est explicitée au 2° de l'article 70-1 relatif à la liste des traitements concernés.

Ces règles sont la transposition de l'article 3 de la directive.

• Traitements de données sensibles à des fins pénales (article 70–2)

Le traitement, à des fins pénales, de données sensibles au sens du I de l'article 8 de la loi de 1978 [(2)] ne sera possible qu'à **trois conditions cumulatives** :

— en cas de « *nécessité absolue* » ;

— sous réserve de garanties appropriées pour les droits et libertés de la personne concernée ;

— à condition d'être autorisé par un acte législatif ou réglementaire, d'avoir pour objet de protéger les intérêts vitaux d'une personne physique ou de porter sur des données manifestement rendues publiques par la personne.

Ces dispositions sont la transposition de l'article 10 de la directive.

---

(1) Avis du Conseil d'État (n° 393836) sur 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, 7 décembre 2017, § 8.

(2) Voir supra*, le commentaire de l'article 7.*

- Formalités préalables pour les traitements mis en œuvre pour le compte de l'État (article 70-3)

L'exigence de formalités préalables est conservée pour les traitements de données personnelles en matière pénale mis en œuvre pour le compte de l'État dans les conditions prévues aux articles 26 et 28 à 31 de la loi de 1978 :

— un **arrêté du ministre compétent, pris après avis motivé et publié de la CNIL,** devra autoriser les traitements mis en œuvre pour le compte de l'État, comme le prévoit aujourd'hui le I de l'article 26 de la loi de 1978 ;

— un **décret en Conseil d'État pris après avis motivé et publié de la CNIL** restera nécessaire pour ceux de ces traitements qui comportent des **données sensibles**, comme en dispose déjà le II du même article 26.

La possibilité laissée aux États de prévoir un encadrement plus rigoureux pour certaines catégories de traitements en matière pénale est prévue à l'article 1er, § 3, de la directive.

- Analyse d'impact et consultation préalable (article 70-4)

Est inscrite dans notre droit l'exigence européenne nouvelle d'une **analyse d'impact** relative à la protection des données à caractère personnel ***« si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »***, notamment parce qu'il porte sur des données sensibles.

Cette analyse devra être adressée à la CNIL en même temps que la demande d'avis pour les traitements mis en œuvre pour le compte de l'État, qui restent en effet soumis à autorisation par un acte réglementaire pris après avis de la CNIL.

Pour les traitements non mis en œuvre pour le compte de l'État, comme ceux pratiqués par la SNCF ou la RATP pour le traitement des données collectées par les caméras piétons des agents de sécurité interne, la **consultation de la CNIL** sera **obligatoire** préalablement à la mise en œuvre du traitement « *soit lorsque l'analyse d'impact (...) indique que le traitement présenterait un* ***risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque*** », « *soit lorsque* ***le type de traitement****, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures,* ***présente des risques élevés*** *pour les libertés et les droits des personnes concernées* ».

Il s'agit de la transposition des articles 27 et 28 de la directive.

- Traitements ultérieurs à d'autres fins que celles autorisant la mise en œuvre du traitement à des fins pénales (article 70-5)

Par principe, les traitements ultérieurs à des fins autres que les finalités limitativement prévues par la directive seront **prohibés sauf si des dispositions législatives ou réglementaires nationales ou le droit de l'Union le permet**.

Si une telle autorisation est prévue, **c'est le règlement général sur la protection des données qui s'appliquera**, tout comme il régira l'activité des autorités compétentes pour des missions relevant d'autres finalités que celles prévues pour les traitements relevant de la directive. Toutefois, l'application du règlement sera écartée si le traitement ultérieur ou l'activité de l'autorité compétente relevant d'autres finalités ne rentre pas dans le champ du droit de l'Union.

En cas de transfert à un tiers des données d'un traitement soumis à des conditions spécifiques, l'autorité compétente devra informer le destinataire des données de ces conditions et de l'obligation de les respecter. Si cette transmission a lieu vers un tiers dans un État membre de l'Union européenne ou dans le cadre de la coopération judiciaire en matière pénale ou policière au sein de l'Union, ces conditions spécifiques ne pourront pas être différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État dont relève l'autorité compétente qui transmet les données.

Ces dispositions transposent l'article 9 de la directive.

- Traitements ultérieurs à d'autres fins que celles à l'origine de la collecte des données (articles 70-6 et 70-7)

Les traitements ultérieurs à des fins relevant de la directive sur les traitements de données personnelles en matière pénale mais autres que celles ayant justifié la collecte initiale des données seront en revanche **autorisés**, sous réserve de respecter le chapitre I^{er}, relatif aux principes et définitions, et le nouveau chapitre XIII de la loi de 1978.

Parmi les traitements concernés figurent notamment les traitements de données aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière ou d'exécution de sanctions pénales qui comprennent l'archivage dans l'intérêt public ou à visées scientifiques, statistiques ou historiques. De tels traitements devront être mis en œuvre en respectant les conditions fixées à l'article 36 de la loi de 1978 dans sa rédaction résultant du présent projet de loi [(1)].

Ces règles sont la transposition de l'article 4, § 2 et 3, de la directive.

---

(1) Voir supra*, le commentaire de l'article 12.*

- Distinction entre les données personnelles fondées sur des faits et celles fondées sur des appréciations personnelles (article 70-8)

Les données à caractère personnel figurant dans les traitements en matière pénale mis en œuvre par les autorités compétentes devront, « *dans la mesure du possible* », distinguer celles qui sont fondées sur des faits de celles qui reposent sur des appréciations personnelles.

Il s'agit de la transposition de l'article 7, § 1, de la directive. Cette règle est l'une des traductions du principe d'**exactitude des données**, principe fondateur du droit de la protection des données personnelles [(1)].

- Décisions individuelles automatisées (article 70-9)

Les **interdictions de l'article 10 de la loi de 1978** relatives aux décisions individuelles automatisées sont rendues applicables aux traitements de données personnelles en matière pénale. Il s'agit d'interdire toute décision de justice impliquant une appréciation sur le comportement d'une personne fondée sur un traitement destiné à évaluer certains aspects de sa personnalité, ainsi que toute autre décision produisant des effets juridiques à l'égard d'une personne et fondée exclusivement sur un traitement destiné à établir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Par ailleurs, « *tout **profilage** qui entraîne une discrimination à l'égard des personnes physiques* » sur la base de données sensibles est interdit.

Cet encadrement résulte de la transposition de l'article 11 de la directive.

- Traitements effectués par un sous-traitant (article 70-10)

Les sous-traitants effectuant un traitement de données personnelles en matière pénale seront soumis à certaines exigences :

— s'appliqueront à eux les **exigences posées par la directive qui sont identiques à celles prévues par le règlement général sur la protection des données**, par envoi à l'article 28, § 1, 2, 9 et 10, ainsi qu'à l'article 29 de ce règlement [(2)] ;

— l'obligation pour le sous-traitant de « *présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement (…) garantisse la protection des droits de la personne concernée* » doit s'entendre comme respectant les exigences du chapitre XIII de la loi de 1978 ;

---

(1) Qui figure au 4° de l'article 6 de la loi de 1978 et au d) *du 1 de l'article 4 de la directive.*

(2) Il s'agit de l'interdiction pour le sous-traitant de recruter un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement, la présentation sous une forme écrite, y compris sous format électronique, du contrat ou de l'acte juridique liant le responsable du traitement au sous-traitant ou un sous-traitant à un autre sous-traitant et la mise en cause de la responsabilité du sous-traitant s'il détermine lui-même les finalités et les moyens du traitement.

— **le traitement par un sous-traitant devra être régi par un contrat ou tout autre acte juridique** dont le contenu devra être précisé par décret en Conseil d'État pris après avis de la CNIL. Ce contrat ou cet acte, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet, la durée, la nature et la finalité du traitement, le type de données collectées et les catégories de personnes concernées, les obligations et les droits du responsable du traitement ainsi que l'obligation pour le sous-traitant d'agir sur instruction du responsable.

Ces dispositions sont la transposition des articles 22 et 23 de la directive

ii. Obligations des autorités compétentes et responsables de traitements

- Veiller à la fiabilité des données transmises ou mises à disposition (article 70-11)

Les autorités compétentes devront prendre « *toutes les mesures raisonnables pour* ***garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition*** » :

— en s'assurant, « *dans la mesure du possible* », de la qualité de ces données avant transmission ou mise à disposition ;

— en ajoutant les informations qui permettront au destinataire des données de juger de l'exactitude, de l'exhaustivité, de la fiabilité et du niveau de mise à jour des données.

En cas de transmission de données inexactes ou de manière illicite, le destinataire devra être informé « *sans retard* » en vue de la rectification ou de l'effacement des données concernées ou de la limitation du traitement.

Ces dispositions transposent l'article 7, § 2 et 3, de la directive.

- Distinguer clairement les données de différentes catégories de personnes concernées (article 70-12)

Le responsable du traitement devra établir, « *dans la mesure du possible* », une distinction claire entre les données de différentes catégories de personnes, en particulier entre celles relatives aux **personnes mises en cause**, celles des **personnes reconnues coupables** d'une infraction pénale, celles des **victimes** et celles des **tiers** à une infraction pénale, comme les témoins.

Cette obligation est la transposition de l'article 6 de la directive.

- Garantir l'intégrité et la sécurité des données (article 70-13)

De manière générale, les responsables de traitements devront mettre en œuvre un certain nombre de **« *mesures (…) appropriées afin de garantir un niveau de sécurité adapté au risque* »**, en particulier lorsqu'est en cause un

traitement de données sensibles. Ces mesures, énoncées par la directive, sont identiques à celles prévues par les articles 24 et 25, § 1 et 2, du règlement général sur la protection des données, auxquels il est donc renvoyé [(1)]. Est ajoutée l'obligation de déployer de telles mesures lorsqu'est en cause un traitement de données sensibles, ce qui constitue une nouveauté dans la loi de 1978 et ce que prévoit spécifiquement la directive, à la différence du règlement (**I**).

Par ailleurs, est inscrite dans notre droit la liste des **dix mesures que la directive met à la charge du responsable du traitement et destinées à garantir (II)** :

— le **contrôle de l'accès aux installations** utilisées pour le traitement (**1°**) ;

— le **contrôle des supports de données** contre toute lecture, copie, modification ou suppression non autorisées (**2°**) ;

— le **contrôle de la conservation des données** contre toute introduction non autorisée de données dans le fichier et toute inspection, modification ou effacement non autorisés de données déjà enregistrées (**3°**) ;

— le **contrôle des utilisateurs** afin d'empêcher l'utilisation des données par des personnes non autorisées (**4°**) ;

— le **contrôle de l'accès aux données** pour garantir l'accès des personnes autorisées à utiliser le fichier aux seules données sur lesquelles porte leur autorisation (**5°**) ;

— le **contrôle des modalités de transmission des données** (**6°**) ;

— le **contrôle de l'introduction des données** dans le fichier afin de connaître les données introduites, l'identité de la personne qui y a procédé et le moment de l'introduction (**7°**) ;

— le **contrôle du transport** contre toute lecture, copie, modification ou suppression non autorisées de données lors d'une transmission de données ou du transport de supports de données (**8°**) ;

— la **restauration du système** en cas d'interruption (**9°**) ;

— la **fiabilité et** l'**intégrité du système** face aux éventuels dysfonctionnements de celui-ci (**10°**).

---

(1) Il s'agit des mesures techniques et organisationnelles appropriées, le cas échéant réexaminées et actualisées, pour s'assurer et être en mesure de démontrer que le traitement est conforme à la réglementation, y compris par la mise en œuvre de politiques appropriées en matière de protection des données de la part du responsable du traitement lorsque cela est proportionné au regard des activités de traitement, mais aussi des mesures de protection des données dès la conception et par défaut.

L'ensemble de ces obligations, issues de la transposition des articles 19, 20 et 29 de la directive, sont également applicables aux sous-traitants.

- Tenir un registre des activités de traitement effectuées (article 70-14)

Le responsable du traitement ou le sous-traitant devront tenir un **registre écrit**, y compris électronique, **des activités de traitement** et le mettre **à la disposition de la CNIL**, dans les conditions prévues, de manière identique à la directive, par l'article 30, § 1 à 4, du règlement général sur la protection des données, auquel il est logiquement fait référence.

Informations devant figurer dans le registre des activités de traitement

1. Registre du responsable du traitement

– les nom et coordonnées du responsable du traitement et, le cas échéant, ceux du responsable conjoint, du représentant du responsable et du délégué à la protection des données ;

– les finalités du traitement ;

– la description des catégories de personnes concernées et de données collectées ;

– les catégories de destinataires auxquels les données sont ou vont être communiquées ;

– le cas échéant, les transferts de données vers un pays tiers ou une organisation internationale et, si nécessaire, les documents attestant de l'existence de garanties appropriées ;

– « *dans la mesure du possible* », les délais d'effacement des différentes catégories de données et la description générale des mesures de sécurité techniques et organisationnelles destinées à garantir un niveau de sécurité adapté au risque.

2. Registre du sous-traitant

– les nom et coordonnées du ou des sous-traitants et de chaque responsable de traitement et, le cas échéant, ceux du représentant du responsable ou du sous-traitant et du délégué à la protection des données ;

– les catégories de traitement effectués pour le compte de chaque responsable de traitement ;

– le cas échéant, les transferts de données vers un pays tiers ou une organisation internationale et, si nécessaire, les documents attestant de l'existence de garanties appropriées ;

– « *dans la mesure du possible* », la description générale des mesures de sécurité techniques et organisationnelles destinées à garantir un niveau de sécurité adapté au risque.

La directive prévoyant également des dispositions spécifiques distinctes de celles du règlement, il est précisé que le registre devra contenir « *la description générale des mesures visant à garantir un niveau de sécurité adapté au risque* », notamment en ce qui concerne les traitements de données sensibles, « *l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données (...) sont destinées et, le cas échéant, le recours au profilage* ».

Il s'agit de la transposition de l'article 24 de la directive.

- Tenir un journal de certaines opérations de traitement (article 70-15)

En outre, le responsable de traitement ou le sous-traitant devra établir, pour chaque traitement, « *un* ***journal des opérations de collecte, de modification, de consultation, de communication****, y compris les transferts, l'interconnexion et l'effacement* » **des données** afin d'en établir le motif, la date et l'heure et, « *dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et leurs destinataires* ».

Mis à la disposition de la CNIL, ce journal a pour vocation exclusive de vérifier la licéité du traitement, la capacité d'autocontrôle de celui-ci par le responsable, l'existence de garanties en termes d'intégrité et de sécurité des données ainsi qu'à des fins de procédure pénale.

Cette obligation est issue de la transposition de l'article 25 de la directive.

- Coopérer avec la CNIL et informer sur les violations de données personnelles (article 70-16)

Sont rendus applicables aux responsables de traitements et, le cas échéant, aux sous-traitants mettant en œuvre un traitement de données en matière pénale, d'une part, l'**obligation générale de coopération avec la CNIL** et, d'autre part, les **obligations d'information en cas de violation de données personnelles**. L'obligation de **notification à la CNIL** « *à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et libertés d'une personne physique* » et l'obligation de **communication à la personne concernée en cas de « *risque élevé* »** pour ces droits et libertés étant prévues de manière identique par le règlement général sur la protection des données, il est renvoyé aux articles 31, 33 et 34 de ce règlement.

Les obligations d'information en cas de violation de données personnelles

1. Notification à l'autorité de contrôle

L'obligation de notification s'applique au responsable de traitement à l'égard de la CNIL pour toute violation de données personnelles « *à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et libertés d'une personne physique* » et au sous-traitant à l'égard du responsable du traitement pour toute violation.

La notification à la CNIL doit intervenir dans les 72 heures ; à défaut, elle doit être accompagnée des motifs du retard.

La notification doit décrire la nature de la violation (notamment les catégories et le nombre approximatif de personnes et d'enregistrements de données concernés), communiquer les nom et coordonnées du délégué à la protection des données ou de tout autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, et décrire les conséquences probables de la violation ainsi que les mesures prises ou envisagées pour y remédier ou atténuer les conséquences négatives éventuelles.

Le responsable du traitement peut communiquer ces informations de manière échelonnée dans le temps s'il n'est pas possible de le faire en même temps que la notification. Il doit documenter toute violation, « *en indiquant les faits concernant la violation (...), ses effets et les mesures prises pour y remédier* » afin que l'autorité de contrôle soit en mesure de vérifier le respect de la législation en la matière.

2. Communication à la personne concernée

L'obligation de communication dans les meilleurs délais à la personne concernée ne s'applique que si la violation « *est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* ».

Elle n'est pas nécessaire :

– si le responsable du traitement a mis en œuvre des mesures de protection techniques et organisationnelles appropriées et appliquées aux données concernées par la violation, en particulier des mesures de chiffrement ;

– si le responsable du traitement a pris des « *mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés (...) n'est plus susceptible de se matérialiser* » ;

– si elle exigerait des efforts disproportionnés, auquel cas une communication publique peut être privilégiée.

Elle doit décrire, en termes clairs et simples, la nature de la violation et contenir au moins les nom et coordonnées du délégué à la protection des données ou de tout autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, les conséquences probables de la violation ainsi que les mesures prises ou envisagées pour y remédier ou atténuer les conséquences négatives éventuelles.

La CNIL, après vérification de la gravité de la violation, peut ordonner au responsable du traitement de procéder à cette communication ou décider qu'elle n'est pas nécessaire pour l'un des trois motifs précédemment évoqués.

À ce droit commun de la coopération et de l'information s'ajoutent **deux dispositions spécifiquement prévues par la directive** :

— en cas de violation de données personnelles transmises par le responsable du traitement d'un **autre État membre de l'Union européenne** ou à cet État, les informations relatives à la violation doivent être également communiquées au responsable du traitement de cet État dans les meilleurs délais ;

— **la communication d'une violation à la personne concernée peut être retardée, limitée ou ne pas être délivrée lorsqu'elle est susceptible de compromettre la sécurité publique ou nationale ou les droits et libertés d'autrui ou de faire obstacle au bon déroulement d'une procédure pénale**, à condition que cette dérogation reste nécessaire et proportionnée et tienne compte des droits fondamentaux et des intérêts légitimes de la personne concernée.

Ces dispositions transposent les règles prévues aux articles 30 et 31 de la directive.

- Désigner un délégué à la protection des données (article 70-17)

Le responsable du traitement devra désigner un délégué à la protection des données personnelles, sauf lorsque le traitement est mis en œuvre par une juridiction agissant dans l'exercice de ses fonctions juridictionnelles.

La possibilité prévue, de manière spécifique, par la directive de ne désigner qu'un seul délégué pour plusieurs autorités compétentes, « *compte tenu de leur structure organisationnelle et de leur taille* », est inscrite dans notre droit.

Pour le reste, les dispositions relatives à la désignation, à la fonction et aux missions du délégué prévues par les articles 32 à 34 de la directive sont transposées par renvoi aux dispositions identiques du règlement européen (articles 37, § 5 à 7, 38, § 1 et 2, et 39, § 1) pour ce qui concerne seulement les responsables de traitements [(1)].

Désignation, fonction et missions du délégué à la protection des données

1. Désignation

Le délégué doit être désigné « *sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir* [ses] *missions* ». Il peut être un membre du personnel ou exercer ses missions sur la base d'un contrat de service. Ses coordonnées doivent être publiées et communiquées à la CNIL.

2. Fonction

Le délégué doit être associé, « *d'une manière appropriée et en temps utile* », à toutes les questions relatives à la protection des données personnelles. Le responsable du traitement doit l'aider à exercer ses missions « *en fournissant les ressources nécessaires (...) ainsi que l'accès aux données (...) et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées* ».

3. Missions

Le délégué a quatre missions principales :

– informer et conseiller le responsable du traitement et ses employés sur leurs obligations en matière de protection des données ;

– contrôler le respect de la législation relative à la protection des données personnelles et des règles internes du responsable ;

– délivrer des conseils, sur demande, au moment de l'élaboration de l'analyse d'impact relative à la protection des données personnelles et en vérifier l'exécution ;

– coopérer avec la CNIL et faire office de point de contact avec celle-ci.

Il s'agit de la transposition des articles 32 à 34 de la directive.

(1) La directive, à la différence de certaines dispositions du règlement, ne rend pas ces règles applicables aux sous-traitants.

iii. Droits de la personne concernée

- Droit à l'information de la personne concernée (article 70-18)

Il est créé un droit à l'information impliquant que le responsable du traitement mette à disposition de la personne concernée un socle d'informations, complété, « *dans des cas particuliers* », par des informations supplémentaires destinées à lui permettre d'exercer ses droits. Les dérogations et restrictions actuellement prévues aux V et VI de l'article 32 de la loi de 1978 pour les traitements relevant de la directive sont levées par l'article 18 du projet de loi [(1)].

Liste des informations devant être mises à la disposition de la personne concernée

1. Informations minimales obligatoirement communiquées

– l'identité et les coordonnées du responsable du traitement, et le cas échéant celles de son représentant ;

– le cas échéant, les coordonnées du délégué à la protection des données ;

– les finalités poursuivies par le traitement auquel les données sont destinées ;

– le droit d'introduire une réclamation auprès de la CNIL et les coordonnées de celle-ci ;

– l'existence du droit de demander au responsable du traitement l'accès aux données, leur rectification ou leur effacement, et la limitation du traitement.

2. Informations additionnelles susceptibles d'être communiquées « *dans des cas particuliers (…) afin de lui permettre d'exercer ses droits* »

– la base juridique du traitement ;

– la durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

– le cas échéant, les catégories de destinataires des données, y compris dans les États non membres de l'UE ou au sein d'organisations internationales ;

– au besoin, des informations complémentaires, en particulier lorsque les données sont collectées à l'insu de la personne concernée.

Cette disposition transpose l'article 13 de la directive.

- Droit d'accès de la personne concernée (article 70-19)

Le droit d'accès de la personne au traitement de données qui la concernent, dont le contenu actuel est quelque peu différent de celui prévu par la directive [(2)], est mis en parfaite conformité les exigences de cette dernière.

---

(1) Voir supra*, le commentaire de l'article 18.*

(2) Le droit actuel ne prévoit pas la communication de la base juridique du traitement, de la durée de conservation des données, de la possibilité de demander la rectification ou l'effacement des données et la limitation du traitement ou du droit d'introduire un recours devant la CNIL.

La personne aura le **droit d'obtenir « *la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données* » ainsi qu'à certaines informations limitativement énumérées** [(1)].

Cet article met notre droit en conformité avec l'article 16 de la directive.

- Droit de rectification ou d'effacement des données et de limitation du traitement (article 70-20)

Le nouvel article 70-20 traite des conditions d'exercice du **droit de rectification ou d'effacement des données et de limitation du traitement**.

Le **I** décrit le **contenu** de ce droit qui revêt, pour la personne concernée, trois dimensions principales :

— le **droit à la rectification**, « *dans les meilleurs délais* », **des données** personnelles la concernant qui sont **inexactes** (**1°**) ;

— le **droit de voir ses données complétées**, le cas échéant en transmettant au responsable du traitement une déclaration complémentaire (**2°**) ;

— le **droit à l'effacement**, « *dans les meilleurs délais* », des données personnelles la concernant lorsque le traitement ne respecte pas la législation ou « *lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement* » (**3°**).

Le **II** impose au responsable du traitement de justifier qu'il a procédé aux rectifications, compléments et effacements demandés « *lorsque l'intéressé en fait la demande* ».

Le **III** dispose que **lorsqu'il ne peut être déterminé si les données sont exactes ou non ou lorsqu'elles doivent être conservées à des fins probatoires, le responsable du traitement ne procède pas à l'effacement sollicité mais limite le traitement**.

Le **IV** exige du responsable du traitement qu'il informe la personne concernée de tout refus de rectifier ou d'effacer les données ou de limiter le traitement ainsi que des motifs du refus.

Les **V et VI** prévoient une **obligation de notification du responsable du traitement** :

---

(1) Les finalités et la base juridique du traitement, les catégories de données concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées, la durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée, la possibilité de demander au responsable la rectification ou l'effacement des données relatives à la personne ou de limiter le traitement de ses données, le droit d'introduire une réclamation auprès de la CNIL avec les coordonnées de celle-ci ainsi que la communication des données en cours de traitement et toute information disponible quant à leur source.

— à l'autorité compétente dont proviennent les données inexactes à rectifier (**V**) ;

— aux destinataires susceptibles d'être concernés par des données à rectifier, compléter ou effacer ou de limiter le traitement afin qu'ils procèdent aux mêmes diligences pour le traitement des données placées sous leur responsabilité (**VI**).

Ces dispositions sont la transposition de l'article 16 de la directive.

- Gratuité des informations transmises à la personne concernée (article 70-23)

Il est prévu que, par principe, **toutes les informations transmises à la personne concernée en vertu des droits qui lui sont reconnus devront l'être de manière gratuite**, **« *sauf en cas de demande manifestement infondée ou abusive* »**. Dans ce dernier cas, le responsable du traitement pourra exiger le paiement d'une somme ou refuser de donner suite à la demande, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombant au responsable.

Cette règle est la transposition du principe de gratuité fixé par l'article 12, § 4, de la directive.

Enfin, la directive laisse aux États la possibilité de prévoir des règles spécifiques pour l'exercice des droits de la personne concernée afin de tenir compte des impératifs en matière de sécurité ou de préservation de l'efficacité des procédures judiciaires. Le Gouvernement a fait le choix d'utiliser deux de ces possibilités, qui sont l'objet des articles 70-21 et 70-22 d'une part, et de l'article 70-24 d'autre part.

- Restriction des droits de la personne concernée (articles 70-21 et 70-22)

En premier lieu, la directive permet aux États d'adopter des **mesures restreignant les droits de la personne concernée** « *dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée* » afin de ne pas nuire à la prévention ou à la détection d'infractions pénales et de protéger la sécurité et les droits et libertés d'autrui.

Ces restrictions sont prévues, pour le droit à l'information, le droit d'accès ainsi que les droits de rectification ou d'effacement des données et de limitation du traitement, respectivement aux articles 13, § 3, 15, § 1 et 16, § 4 de la directive.

Le Gouvernement ayant fait le choix d'utiliser la marge d'appréciation laissée par la directive, le **nouvel article 70-21** inscrit dans notre droit les conditions de restriction posées par celle-ci.

Le **I** reprend les **cinq finalités légitimes** de telles restrictions :

— éviter de gêner des enquêtes ou procédures judiciaires (1°) ou de nuire à la prévention ou à la détection d'infractions pénales et à l'exécution de sanctions pénales (2°) ;

— protéger la sécurité publique (3°) ou la sécurité nationale (4°) ;

— garantir les droits et libertés d'autrui (5°).

L'acte instaurant le traitement – pour les traitements mis en œuvre pour le compte de l'État, l'arrêté ou le décret en Conseil d'État pris après avis de la CNIL – devra prévoir les restrictions. Le choix de prévoir ces restrictions dans l'acte constitutif se justifie par le maintien de formalités préalables pour les traitements concernés, permettant une détermination *in concreto* des limitations appropriées à apporter aux droits de la personne.

Les **II et III** prévoient que les restrictions pourront consister, pour le responsable du traitement :

— à **retarder ou limiter la fourniture des informations supplémentaires susceptibles d'être transmises à la personne concernée** en vertu du II de l'article 70-18, **ou à ne pas les fournir (1° du II)** ;

— à **limiter, en totalité ou en partie, le droit d'accès (2° du II)** : dans ce cas, le responsable du traitement devra en informer la personne dans les meilleurs délais ainsi que des motifs du refus ou de la limitation, à moins que la communication de ces informations risque de compromettre l'une des cinq finalités justifiant la restriction ; en tout état de cause, le responsable devra consigner les motifs de fait ou de droit sur lesquels se fonde sa décision et les mettre à la disposition de la CNIL (**III**) ;

— à **ne pas informer la personne de son refus de rectifier ou d'effacer les données la concernant ou de limiter le traitement**, ainsi que des motifs de cette décision (**3° du II**).

Quoi qu'il en soit, la personne concernée doit être informée par le responsable du traitement de la **possibilité d'exercer ses droits par l'intermédiaire de la CNIL ou de former un recours juridictionnel (IV).** Permettre à la personne d'exercer ses droits, par l'intermédiaire de l'autorité de régulation, en cas de restriction est une exigence posée par l'article 17 de la directive qu'il convient de transposer.

Tel est l'objet du **nouvel article 70-22** qui, dans cette hypothèse, rend applicable la législation en vigueur en cas de saisine de la CNIL pour l'exercice des droits de la personne concernée par un traitement intéressant la sûreté de l'État, la défense ou la sécurité publique, à savoir les deuxième et troisième alinéas de l'article 41 de la loi de 1978.

Modalités d'exercice indirect des droits de la personne concernée en cas de restriction (deuxième et troisième alinéas de l'article 41 de la loi du 6 janvier 1978)

La demande est adressée à la CNIL qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour « *mener les investigations utiles et faire procéder aux modifications nécessaires* ». Celui-ci peut se faire assister d'un agent de la CNIL. Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque la CNIL constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque la CNIL informe la personne qu'elle a procédé aux vérifications nécessaires, elle devra également l'informer de son droit de former un recours juridictionnel.

- Données figurant dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale (article 70-24)

L'article 18 de la directive laisse aux États membres la possibilité de conserver des règles nationales spécifiques pour l'exercice des droits de la personne concernée par des données personnelles figurant dans une décision judiciaire, un casier ou un dossier judiciaire et traitées dans le cadre d'une procédure pénale.

Le Gouvernement ayant fait le choix d'utiliser cette marge d'application, le nouvel article 70-24 prévoit que **les règles précédemment mentionnées relatives aux droits de la personne ne s'appliquent pas en pareil cas** et que l'accès aux données la concernant se fait dans les conditions prévues par le code de procédure pénale.

iv. Transferts de données hors de l'UE

La directive, qui encadre pour la première fois au niveau européen le transfert vers des pays tiers de données en matière pénale [(1)], constitue une **clarification utile du cadre juridique actuel**. Elle distingue **deux types de transferts** :

— ceux **vers une autorité compétente** [(2)] d'un pays tiers **(articles 35 à 38)** : ces transferts seront possibles soit en présence d'une décision d'adéquation

(1) Auparavant, seule la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale posait des restrictions aux transferts internationaux de données en matière pénale, mais uniquement s'agissant de données provenant d'autres États membres de l'Union européenne.

(2) C'est-à-dire une autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales ainsi que tout organisme à qui l'exercice de l'autorité publique et des prérogatives de puissance publique à ces mêmes fins a été confié.

de la Commission européenne ou de garanties appropriées, soit, en l'absence d'une telle décision ou de telles garanties, pour la poursuite de certaines finalités ;

— ceux **directement vers des « destinataires »** établis dans un pays tiers, principalement des services de communications électroniques délocalisés à l'étranger et qui servent souvent à la commission d'infractions **(article 39)**.

Les **nouveaux articles 70-25 à 70-27** transposent ces dispositions.

- Transferts de données vers un État en présence d'une décision d'adéquation de la Commission européenne ou de garanties appropriées (article 70-25)

Le transfert de données personnelles en matière pénale vers un État n'appartenant pas à l'UE ou une organisation internationale ne sera possible qu'à **quatre conditions cumulatives**.

En premier lieu, un tel transfert devra être **nécessaire à l'une des finalités pour lesquelles les données ont été collectées en France**, à savoir la prévention et la détection des infractions pénales, les enquêtes et poursuites en la matière ou l'exécution de sanctions pénales (**1°**).

En deuxième lieu, les données devront être transférées **à une personne qui est une autorité compétente** au sens de l'article 70-1 **chargée de l'une de ces finalités** (**2°**).

En troisième lieu, **dans le cas de données provenant d'un autre État, l'État qui a transmis ces données devra préalablement autoriser ce transfert** conformément à son droit national ; si cette autorisation préalable ne peut pas être obtenue en temps utile, le transfert ne sera possible que s'il « *est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre État ou pour la sauvegarde des intérêts essentiels de la France* » et sous réserve d'une information « *sans retard* » de l'État qui a transmis ces données (**3°**).

En dernier lieu, il devra exister **une décision d'adéquation** de la Commission européenne **ou, à défaut d'une telle décision, « *des garanties appropriées* *en ce qui concerne la protection des données à caractère personnel (...)* *dans un instrument juridique contraignant*** » (conventions mises en œuvre avec cet État, dispositions juridiquement contraignantes exigées à l'occasion d'échanges de données…). **À défaut d'une telle décision ou de telles garanties, « *le responsable du traitement* [aura] *évalué toutes les circonstances du transfert et estime*[ra] *qu'il existe des garanties appropriées* *au regard de la protection des données à caractère personnel* » (**4°**).

La décision d'adéquation de la Commission européenne (article 36 de la directive)

La décision d'adéquation est une décision prise par la Commission européenne, par laquelle elle constate « *que* ***le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat*** » au regard notamment des éléments suivants :

– l'État de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire ces personnes ;

– l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise ;

– et les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants et de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

L'existence d'une telle décision, qui présente des garanties spécifiques, **dispense en conséquence d'autorisation spécifique le transfert de données personnelles en matière pénale vers des pays tiers**.

La décision est soumise à un « *mécanisme d'**examen périodique**, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale* ».

Lorsque les informations disponibles révèlent que le pays, le secteur ou l'organisation internationale n'assurent plus un niveau de protection adéquat, la Commission abroge, modifie ou suspend la décision d'adéquation.

Dans le cas de **transferts décidés sur le seul fondement d'une évaluation par le responsable de traitement des circonstances du transfert et du constat qu'il existe des garanties appropriées**, le responsable sera soumis à un certain nombre d'**obligations (dixième et avant-dernier alinéas)** :

— en aviser la CNIL, sauf s'il s'agit d'une juridiction agissant dans le cadre de ses activités juridictionnelles ;

— conserver la date et l'heure du transfert, les informations sur l'autorité compétente destinataire ainsi que la justification du transfert et des données transférées, l'ensemble de ces informations devant être mis à la disposition de l'autorité de contrôle à sa demande.

Un transfert décidé sur la base d'une décision d'adéquation ultérieurement abrogée, modifiée ou suspendue par la Commission européenne pourra se poursuivre « *si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument contraignant ou*

[si le responsable du traitement] *estime (…) qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel* » (**dernier alinéa**).

Ce nouveau cadre juridique est la transposition des articles 35 à 37 de la directive.

- Transferts de données vers un État en l'absence de décision d'adéquation ou de garanties appropriées (article 70-26)

Le transfert de données vers un État tiers en l'absence de décision d'adéquation ou de garanties appropriées en matière de protection de la vie privée ne sera possible qu'à condition qu'il soit **nécessaire à l'une des cinq finalités suivantes** :

— la **sauvegarde des intérêts vitaux d'une personne (1°) ou des intérêts légitimes de la personne concernée** lorsque le droit français le prévoit (**2°**) : dans ce cas, le responsable du traitement devra conserver la date et l'heure du transfert, les informations sur l'autorité compétente destinataire ainsi que la justification du transfert et des données transférées, l'ensemble de ces informations devant être mise à la disposition de l'autorité de contrôle à sa demande (**dernier alinéa**) ;

— pour **prévenir une menace grave et immédiate pour la sécurité publique** d'un État membre de l'UE ou d'un pays tiers (**3°**) ;

— pour **faciliter, « *dans des cas particuliers* », la prévention et la détection des infractions pénales, les enquêtes et poursuites en la matière ou l'exécution de sanctions pénales (4°)** ;

— pour **permettre, « *dans un cas particulier* », la constatation, l'exercice ou la défense de droits en justice** en rapport avec les mêmes fins (**5°**).

Dans ces deux derniers cas, le responsable ne transfère pas les données « *s'il estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public* » (**avant-dernier alinéa**).

Ces dispositions transposent l'article 38 de la directive.

- Transferts de données à des destinataires établis dans des pays tiers (article 70-27)

Les transferts de données vers des destinataires établis dans des pays tiers autres que les autorités compétentes visent, à titre principal, le cas des services de communications électroniques délocalisés à l'étranger tels que les fournisseurs d'accès à internet dont la coopération est utile pour la communication d'adresses IP, de pseudonymes ou d'adresses de messagerie nécessaires à la répression d'infractions pénales commises sur les réseaux.

Ce type de transferts ne sera possible qu'**à condition, d'une part, que la législation applicable aux traitements de données personnelles en matière pénale soit respectée et, d'autre part, que cinq conditions soient remplies** :

— le transfert devra être **nécessaire à l'exécution de la mission de l'autorité** qui transfère les données (**1°**) ;

— l'autorité qui transmet les données devra établir « *qu'il n'**existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public** nécessitant le transfert* » (**2°**) ;

— elle estimera que **le transfert à l'autorité compétente de l'État est inefficace ou inapproprié**, « *notamment parce que le transfert ne peut pas être effectué en temps opportun* » (**3°**) ;

— **l'autorité compétente de l'autre État devra être informée « *dans les meilleurs délais* » (4°)** ;

— l'autorité qui transmet les données devra **informer le destinataire de la ou des finalités pour lesquelles les données transmises doivent exclusivement faire l'objet d'un traitement**, « *à condition qu'un tel traitement soit nécessaire* » (**5°**).

En toute hypothèse, l'autorité qui transmet les données devra informer la CNIL du transfert opéré et conserver la date et l'heure du transfert, les informations sur le destinataire ainsi que la justification du transfert et les données transférées (**deux derniers alinéas**).

Se trouvent ainsi transposées dans notre droit les dispositions de l'article 39 de la directive.

c. La position de la Commission

La Commission a approuvé la transposition proposée par le Gouvernement de la directive relative au traitement des données pénales à des fins pénales, en procédant toutefois, à l'initiative de votre rapporteure, à de nombreuses modifications rédactionnelles et clarifications.

Par ailleurs, elle a complété ces dispositions dans trois directions :

— en premier lieu, avec l'avis favorable de votre rapporteure et du Gouvernement, elle a adopté un amendement de Mme Danièle Obono posant, à l'article 70-1, l'exigence de **proportionnalité de la durée de conservation des données traitées**, « *compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions concernées* » ;

— en deuxième lieu, elle a adopté un amendement de votre rapporteure précisant, à l'article 70-21, que **lorsque la restriction porte sur le droit d'information, la personne devra seulement être avisée de la possibilité de**

saisir la CNIL, et non de celle d'exercer un recours, cette dernière obligation incombant, aux termes de la directive et uniquement en cas de restriction du droit d'information, à la CNIL et non au responsable de traitement : cet amendement permet de ne pas sur-transposer le directive et maintient en revanche l'obligation d'informer la personne concernée de la possibilité de former un recours et de saisir la CNIL en cas de restriction des autres droits prévus par la loi (droit d'accès, droit de rectification, droit d'effacement) ;

— en dernier lieu, elle a adopté un amendement de votre rapporteure prévoyant que **les informations communiquées à la personne** concernée devront être **transmises par tout moyen approprié**, de préférence sous la même forme que la demande, **et de manière gratuite**, sauf demande manifestement infondée ou abusive.

*

* *

La Commission examine l'amendement CL41 de Mme Danièle Obono.

Mme Danièle Obono. Pour notre groupe, l'article 19 est l'un des plus problématiques de ce projet de loi, car il permet la généralisation des fichiers en matière pénale, « *à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». De tels fichiers ne devront plus nécessairement être autorisés par arrêté ministériel, comme le prévoit aujourd'hui l'article 26 de la loi du 6 janvier 1978.

A l'instar de la CNIL, qui l'a souligné dans sa délibération du 30 novembre 2017, il nous semble impératif de promouvoir une logique de renforcement du droit commun, plutôt que de démantèlement et de facilitation. La CNIL a relevé que « *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)* ».

C'est pourquoi notre amendement tend à supprimer l'article 19.

Mme la rapporteure. La transposition de la directive renforce, au contraire, l'encadrement des règles applicables aux fichiers de police et de justice. Parmi les progrès réalisés, on peut citer la création d'un droit d'information de la personne, l'exercice en principe direct des droits d'information, d'accès, de rectification, d'effacement et de limitation des données, l'élargissement du champ des obligations à la charge des responsables de traitements et des sous-traitants, ou encore l'amélioration de l'encadrement des transferts internationaux de données. Par conséquent, je donne un avis défavorable.

*La Commission **rejette** l'amendement.*

*Elle **adopte** ensuite l'amendement rédactionnel CL153 de la rapporteure.*

Puis elle en vient à l'amendement CL49 de Mme Danièle Obono.

Mme Danièle Obono. Notre amendement vise à renforcer la protection des droits et la proportionnalité de la réponse étatique. Pour être considérés comme licites, il nous semble que des traitements de données tels que les fichiers pénaux ne doivent pas être seulement « *nécessaires* », mais « *strictement nécessaires* » – il s'agit d'éviter les abus.

Mme la rapporteure. J'émets un avis favorable, à condition que la première partie de l'amendement soit supprimée puisque la précision que vous souhaitez ajouter n'est pas prévue par la directive. La deuxième partie, relative à la proportionnalité de la durée des conservations des données, reprend des principes du RGPD, mais cette précision est néanmoins bienvenue.

Mme la garde des Sceaux. Je suis du même avis : l'adverbe « *strictement* » que vous proposez n'est pas utile ; en revanche, je suis favorable à la seconde partie de l'amendement.

Mme Danièle Obono. Je rectifie l'amendement en ce sens.

*La Commission **adopte** l'amendement **ainsi rectifié.***

*Puis elle **adopte** successivement l'amendement rédactionnel CL154, l'amendement CL156 tendant à corriger une erreur matérielle, les amendements de précision CL157 et CL159, l'amendement CL160 tendant à corriger une erreur de référence, l'amendement de précision CL161, les amendements rédactionnels CL162 à CL172, l'amendement de précision CL173, les amendements rédactionnels CL174, CL175 et CL222, l'amendement de précision CL176, les amendements rédactionnels CL177 à CL180, l'amendement de précision CL181, l'amendement rédactionnel CL182, l'amendement CL183 tendant à corriger une erreur de référence et les amendements rédactionnels CL184 à CL186, tous de la rapporteure.*

Elle examine ensuite l'amendement CL223 de la rapporteure.

Mme la rapporteure. Je vous propose d'apporter une clarification permettant de ne pas surtransposer la directive.

*La Commission **adopte** l'amendement.*

Elle est ensuite saisie de l'amendement CL224 de la rapporteure.

Mme la rapporteure. Il s'agit d'imposer notamment la gratuité de la transmission d'informations à la personne concernée par un traitement de données pénales.

La Commission ***adopte*** *l'amendement.*

Puis elle ***adopte*** *successivement l'amendement rédactionnel CL187, l'amendement CL188 tendant à corriger une erreur de référence, les amendements rédactionnels CL189, CL209, CL190 et CL191, l'amendement de clarification CL221, les amendements rédactionnels CL192 et CL193, les amendements de précision CL194 à CL196 et les amendements rédactionnels CL198 à CL201, tous de la rapporteure.*

Elle ***adopte*** *enfin l'article 19* ***modifié****.*

TITRE IV
HABILITATION À AMÉLIORER L'INTELLIGIBILITÉ DE LA LÉGISLATION APPLICABLE À LA PROTECTION DES DONNÉES

Article 20
Habilitation à réviser par voie d'ordonnance la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Résumé du dispositif et effets principaux :

Le présent article autorise le Gouvernement, dans le respect des dispositions prévues aux titres I à III du présent projet de loi, à prendre par voie d'ordonnance, dans un délai de 6 mois à compter de la publication de la loi, les mesures permettant une remise en forme et en cohérence non seulement de la loi n° 78-17 du 6 janvier 1978 Informatique et Libertés, mais aussi de textes voisins et liés, sans remettre en cause les choix fondamentaux faits dans le projet de loi, de façon à garantir une meilleure accessibilité de l'ensemble du droit applicable au traitement des données personnelles.

Modifications adoptées par la commission des Lois :

Sur proposition de votre rapporteure, la Commission a adopté un amendement de précision relatif à l'application outre-mer du présent article.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés constitue le texte fondateur et unique en matière de protection des données à caractère personnel en France.

La mise en conformité de cette loi avec le « paquet européen » des données à caractère personnel adopté le 27 avril 2016 conduit à intégrer dans ce texte des dispositions qui relèvent de champs d'application différents (règlement (UE) 2016/679 d'une part, directive (UE) 2016/680 d'autre part), tout en maintenant des dispositions qui concernent également des traitements ne relevant pas du droit de l'Union européenne, tels les fichiers relatifs à la défense nationale par exemple.

Les choix légistiques faits par le Gouvernement, validés par le Conseil d'État dans son avis sur le présent projet de loi, tiennent compte à la fois de la nécessité de mettre en œuvre de manière complète le droit de l'Union issu du règlement et de la directive précités et du souhait de conserver comme instrument principal au niveau national la loi du 6 janvier 1978.

Plutôt que de recopier le règlement, le Gouvernement a retenu une approche consistant à n'éliminer de la loi n° 78-17 du 6 janvier 1978 que les dispositions contraires au règlement et à mettre en conformité, notamment sur le plan des définitions, celles qui doivent l'être. Chaque fois que le Gouvernement souhaite utiliser l'une des 56 marges de manœuvre nationales ouvertes par le

règlement, il s'efforce de réécrire les dispositions nécessaires, qu'elles soient plus exigeantes ou au contraire plus souples, plutôt que de répéter le principe posé par le règlement.

Pour autant, des adaptations et coordinations supplémentaires sont indispensables. L'article 21 du présent projet de loi contient déjà certaines mesures de coordination rendues directement nécessaires par les modifications apportées à la loi n° 78-17 en raison de la transposition du règlement et de la directive.

Toutefois, un travail plus ambitieux s'impose pour procéder à une remise en forme et en cohérence non seulement de la loi de 1978, mais aussi de textes voisins et liés, sans remettre en cause les choix fondamentaux faits dans le projet de loi, de façon à garantir une meilleure intelligibilité de l'ensemble du droit applicable au traitement des données personnelles.

C'est la raison pour laquelle l'article 20 autorise le Gouvernement à prendre par voie d'ordonnance, dans un délai de six mois suivant la promulgation de la loi, les mesures qui relèvent du domaine de la loi nécessaires à :

— la réécriture de l'ensemble de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification, à la cohérence et à l'intelligibilité de cette loi consécutive à sa mise en conformité au règlement et à la transposition de la directive telle que résultant de la présente loi ;

— à mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel, apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi, et abroger les dispositions devenues sans objet ;

— à l'adaptation et aux extensions à l'outre-mer des dispositions prévues aux deux points précédents, ainsi qu'à l'application en Nouvelle-Calédonie, à Wallis-et-Futuna, en Polynésie française, à Saint-Barthélemy, à Saint-Pierre-et-Miquelon et dans les Terres australes et antarctique françaises.

Le projet de loi de ratification de l'ordonnance qui sera rédigé par le Gouvernement devra être déposé devant le Parlement dans un délai de six mois (le projet soumis au Conseil d'État prévoyait 18 mois) à compter de la publication de l'ordonnance.

Critiquée par de nombreuses personnes auditionnées par votre rapporteure qui auraient préféré disposer d'un texte clair et complet relatif à la protection des données personnelles en France avant le 25 mai 2018, date à laquelle le règlement et la directive devront être obligatoirement transposés, cette méthode n'en est pas moins parfaitement constitutionnelle.

Le Conseil Constitutionnel considère en effet que le législateur peut autoriser le Gouvernement à tirer les conséquences, par ordonnances, de la loi qu'il a adoptée et assurer ainsi la coordination des dispositions législatives en vigueur avec celles de cette loi. Il juge également de manière constante que « *si l'article 38 de la Constitution fait obligation au Gouvernement d'indiquer avec précision au Parlement, afin de justifier la demande qu'il présente, la finalité des mesures qu'il se propose de prendre par voie d'ordonnance ainsi que leur domaine d'intervention, il n'impose pas au Gouvernement de faire connaître au Parlement la teneur des ordonnances qu'il prendra en vertu de cette habilitation* » [(1)].

Pour autant, votre rapporteure a demandé au Gouvernement de lui faire parvenir dans les meilleurs délais l'état d'avancement de ce projet d'ordonnance afin de pouvoir informer au mieux ses collègues parlementaires et l'ensemble de la société civile quant à son contenu.

*

* *

La Commission examine l'amendement CL42 de M. Ugo Bernalicis.

Mme Danièle Obono. Notre groupe s'oppose à ce que le Gouvernement puisse réécrire par ordonnance la loi du 6 janvier 1978, comme le prévoit l'article 20 : cela témoigne d'une précipitation que le Conseil d'État et la CNIL ont dénoncée, et nous considérons que ce n'est pas à la hauteur du débat nécessaire sur de tels sujets. Notre amendement CL42 propose donc de supprimer l'article.

Mme la rapporteure. Avis défavorable. Je ne suis pas non plus adepte, à titre personnel, du recours aux ordonnances afin de légiférer, mais nous manquons désormais de temps pour respecter les délais fixés au niveau européen. Je comprends les inquiétudes qui se sont fait jour, lors des auditions, sur le manque de lisibilité : je pousse donc le Gouvernement à rédiger l'ordonnance le plus rapidement possible, en précisant que cela ne nous empêchera pas de débattre de la réécriture de la loi de 1978, et ce sur tous les points. J'incite nos collègues à se saisir des différents sujets qui sont concernés et à veiller à ce que l'ordonnance soit rédigée, comme promis, à droit constant.

M. Philippe Gosselin. Cette manière de légiférer par ordonnance est un dessaisissement du Parlement qui devient habituel en ce moment. Dans une autre salle de commission, quelques étages plus haut, onze articles prévoyant des ordonnances ont ainsi été adoptés.

En l'occurrence, je le regrette d'autant plus que nous avions fait le nécessaire sous la législature précédente, avec Anne-Yvonne Le Dain, Cécile Untermaier et d'autres collègues, pour qu'il y ait une sorte de SAV, un « service

(1) Voir par exemple, Conseil constitutionnel, décision du 17 mai 2013, n° 2013-669 DC, cons. 79.

avant vote », grâce à un travail mené avec un peu plus de temps et dans la sérénité. Je ne fais pas de reproche à qui que ce soit sur ce dernier point, car je salue la bonne tenue de nos débats, mais je trouve que nous aurions pu avancer autrement que par ordonnance.

La garde des Sceaux nous a dit hier que ce serait un travail de pure légistique : on légiférera à droit constant, alors que l'on aurait pu en profiter pour procéder à une remise à plat sur un certain nombre de sujets. Nous ne pourrons pas le faire complètement dans le cadre du débat sur l'autorisation donnée au Gouvernement, en vertu de l'article 38 de la Constitution, ni lors de la ratification de l'ordonnance. Je regrette cette occasion manquée.

M. Éric Bothorel. L'exposé sommaire de l'amendement critique une « précipitation d'amateurs » et « un mépris pour un domaine aussi fondamental » : je ne fais pas partie de cette commission, mais je voudrais quand même souligner que nous venons d'examiner le texte pendant une heure et demie sans qu'aucun membre du groupe de La France insoumise ne soit présent, alors que ce groupe appelle au débat… Il est un peu « fort de café » de demander un ralentissement de la procédure et de ne pas être là pour défendre ses propres amendements.

Mme Danièle Obono. C'est la seule et unique fois ! Nous sommes très présents en commission !

Mme Albane Gaillot. Je voudrais insister sur la qualité des débats sur les articles 7, 9 et 13, dont je suis la rapporteure pour avis au nom de la commission des Affaires sociales : nous avons fait plusieurs dizaines d'heures d'auditions qui ont permis d'améliorer le texte sur certains points et surtout d'envisager l'avenir. On ne peut pas dire qu'aucun travail n'a été réalisé, bien au contraire.

Mme la garde des Sceaux. Comme M. Gosselin l'a rappelé, il s'agira d'un travail de pure légistique. C'est ce que dit l'article 20 : l'ordonnance permettra de procéder à la réécriture de l'ensemble de la loi de 1978 avec les corrections formelles et les adaptations nécessaires, « *telles que résultant de la présente loi* ». On s'appuiera sur ce que le Parlement aura adopté dans le cadre du texte dont nous débattons aujourd'hui.

M. Philippe Gosselin. Je ne souhaite maintenant qu'une chose : que le Gouvernement se hâte, et pas lentement. *(Sourires.)* Cela peut sembler contradictoire avec ce que j'ai dit précédemment, mais il n'en est rien : plus vous irez vite, moins il y aura d'ambiguïté et d'incompréhension à cause du décalage entre le RGPD et la loi de 1978 dans sa rédaction actuelle.

La Commission ***rejette*** *l'amendement.*

Puis elle ***adopte*** *l'amendement de précision CL214 de la rapporteure.*

La Commission ***adopte*** *ensuite l'article 20* ***modifié****.*

TITRE V
DISPOSITIONS DIVERSES ET FINALES

Article 21
(art. 15, 16, 29, 30, 31, 39, 67, 70 et 71 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Coordinations

Résumé du dispositif et effets principaux :

Le présent article procède à la suppression des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en contradiction avec les dispositions du « paquet européen » des données à caractère personnel adopté le 27 avril 2016, que sont le règlement (UE) 2016/679 d'une part et la directive (UE) 2016/680 d'autre part en raison de la disparition de certaines formalités préalables en application de l'article 9 du présent projet de loi. Il permet également de procéder à plusieurs coordinations légistiques.

Modifications adoptées par la commission des Lois :

Sur proposition de votre rapporteure, la Commission a adopté un amendement de précision et quatre amendements de coordination.

Le présent article supprime les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en contradiction avec celles du règlement général sur les données personnelles et de la directive relative aux traitements en matière pénale, en raison de la disparition de certaines formalités préalables.

Sont supprimées :

— l'ensemble des références relatives au régime de déclaration préalable d'un traitement à la CNIL résultant de la suppression des articles 22 à 24 de la loi n° 78-17 par l'article 9 du présent projet de loi. Il s'agit des références mentionnées à l'article 15 alinéa 4, au I de l'article 31, au dernier alinéa de l'article 39, au quatrième alinéa de l'article 67, et au premier et troisième alinéa de l'article 70 ;

— l'ensemble des références à l'article 25 relatif aux autorisations préalables de traitement par la CNIL – également abrogé par l'article 9 du présent projet de loi – mentionnées aux articles 16 (troisième alinéa), 29, 30 (I), 31 (I), 67 (premier alinéa), et à la deuxième phrase de l'article 71.

En outre, au cinquième alinéa de l'article 67, relatif au rôle du correspondant appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi, le présent article supprime la sanction applicable jusqu'alors selon

laquelle : « *En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés* ».

Enfin, le présent article modifie le deuxième alinéa de l'article 70 afin de tirer les conséquences de l'article 17 du présent projet de loi en permettant à la CNIL d'obtenir la suspension d'un transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680, dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation.

*

* *

La Commission ***adopte*** *successivement les amendements de coordination CL230, CL233 et CL232, l'amendement de précision CL215 et l'amendement de coordination CL231, tous de la rapporteure, puis l'article 21* ***modifié****.*

Article 22

Mise à disposition du public, dans un format ouvert et aisément réutilisable, de la liste des traitements ayant fait l'objet de formalités préalables

Résumé du dispositif et effets principaux :

Le présent article maintient, pour les traitements ayant fait l'objet de formalités antérieurement à l'entrée en vigueur de la future loi, l'obligation pour la Commission nationale de l'informatique et libertés de mettre à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements arrêtée à cette date, pour une durée de dix ans.

Dernières modifications législatives intervenues :

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 a imposé à la Commission nationale de l'informatique et des libertés de tenir à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26 (traitements dits de « souveraineté » ne faisant pas l'objet d'une publication).

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a fait basculer ce registre des formalités préalables dans l'*open data* en prévoyant une mise à disposition du public, dans un format ouvert et aisément réutilisable.

Modifications adoptées par la commission des Lois :

La Commission a adopté un amendement de précision.

1. L'état du droit

Depuis la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés tient à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26 (traitements dits de « souveraineté » ne faisant pas l'objet d'une publication).

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a fait basculer ce registre des formalités préalables dans l'*open data* en prévoyant une mise à disposition du public dans un format ouvert et aisément réutilisable.

Lorsqu'un responsable de traitement dispose d'un correspondant à la protection des données, ce droit s'exerce directement auprès de ce dernier, qui doit tenir la liste des traitements mis en œuvre (article 22-III de la loi n° 78-17).

Ce droit de communication ne correspond pas au droit d'accès aux documents administratifs prévu par le code des relations entre le public et l'administration dès lors que la liste en question constitue, par nature, un document inachevé, puisqu'il évolue avec les nouvelles formalités préalables qui interviennent auprès de la commission et qu'il contient des données à caractère personnel (identité du responsable de traitement, adresse), deux caractéristiques qui font obstacle au droit à l'accès des documents administratifs.

Le règlement (UE) 2016/679 ne prévoit pas d'obligation de mise à disposition d'un tel registre puisque la logique de responsabilisation qu'il promeut permet la suppression de la grande majorité des formalités préalables et que le droit d'accès apporte une réponse aux personnes concernées désireuses de connaître ces informations (articles 13 et 14).

Pour autant, le règlement ne s'oppose pas non plus à une mesure d'information du public et des personnes concernées, puisque le droit à l'information est une composante majeure de la protection des données à caractère personnel (article 15).

Or, de nombreux traitements en cours se poursuivront après le 25 mai 2018, date d'entrée en application du règlement, de sorte qu'il serait préjudiciable pour le droit à l'information des personnes concernées de ne plus avoir connaissance de l'ensemble des traitements mis en œuvre. Il apparaît dès lors nécessaire de prévoir un nouveau registre des autorisations existantes, en plus des publications officielles.

2. Le dispositif proposé

Le présent article maintient l'obligation pour la CNIL de mettre à la disposition du public, dans un format ouvert et aisément réutilisable, pour une durée de dix ans, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26 (traitements dits de « souveraineté » ne faisant pas l'objet d'une publication).

Ce nouveau registre des autorisations existantes, en plus des publications officielles, constitue un outil pertinent pour les actuels correspondants à la protection des données, et le sera également pour les futurs délégués à la protection des données. Cette disposition apparaît cohérente avec l'article 10 du projet de loi qui prévoit par ailleurs que ce délégué pourra communiquer la liste des traitements effectués par le responsable de traitement qui l'a désigné à toute personne qui lui en fait la demande.

Il s'agit d'une mesure qui contribue à l'exercice effectif du droit à l'information, tant au titre de l'accès à l'information publique pour les traitements mis en œuvre par des administrations, qu'à l'égard des personnes concernées. Les entreprises auront d'ailleurs la possibilité de réutiliser les informations contenues dans ce registre, dans le respect de la loi n° 78-17.

*

* *

La Commission ***adopte*** *l'amendement de précision CL216 de la rapporteure.*

Elle ***adopte*** *ensuite l'article 22* ***modifié****.*

Article 23

(art. 230-8, 230-9 et 804 du code de procédure pénale)

Modalités d'effacement des données inscrites dans les traitements d'antécédents judiciaires

Résumé du dispositif et effets principaux :

Le présent article tire les conséquences de la décision n° 2017-670 QPC du 27 octobre 2017 par laquelle le Conseil constitutionnel a considéré que les dispositions régissant le traitement des antécédents judiciaires (TAJ), en privant les personnes mises en cause dans une procédure pénale autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans ce fichier, portaient une atteinte disproportionnée au droit au respect de la vie privé.

Dernières modifications législatives intervenues :

Le TAJ a été institué par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 ». Son régime a été principalement modifié par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Cette loi a mis notre droit en conformité avec la jurisprudence de la Cour européenne des droits de l'homme, qui, en 2014, avait condamné la France dans l'affaire « Brunet ».

Modifications adoptées par la commission des Lois :

La Commission a approuvé cet article et, sur proposition de votre rapporteure, l'a complété afin d'aligner les délais laissés aux magistrats compétents pour statuer sur les demandes d'effacement qui leur sont adressées.

1. L'état du droit

Succédant en 2012 aux fichiers d'antécédents judiciaires STIC et JUDEX utilisés respectivement par la police et la gendarmerie nationales, le traitement des antécédents judiciaires (TAJ) est un **fichier commun aux services de police et de gendarmerie**.

Institué par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 », en vue de « *faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs* », il est régi par les **articles 230-6 à 230-11 du code de procédure pénale**. Les informations qu'il comporte peuvent également être consultées dans le cadre d'enquêtes administratives [(1)].

Peuvent être inscrites dans ce fichier les données recueillies soit au cours des enquêtes ou instructions concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'État [(2)], soit au cours des procédures de recherche des causes de la mort d'autrui ou d'une disparition (article 230-6).

Trois catégories de personnes peuvent voir leurs données personnelles inscrites à ce fichier (article 230-7) : outre les victimes de ces infractions et les personnes faisant l'objet d'une enquête ou instruction pour recherche des causes

(1) Le TAJ peut ainsi être consulté dans le cadre des enquêtes administratives menées en vue de l'acquisition de la nationalité française et de la délivrance de titres pour les étrangers, de la promotion dans les ordres nationaux et de l'accès à certains emplois, en particulier ceux participant à l'exercice des missions de souveraineté de l'État ou relevant du domaine de la sécurité ou de la défense.

(2) Au titre des infractions punies d'une contravention de la cinquième classe figurent, par exemple, les violences volontaires ayant entraîné une incapacité totale du travail d'une durée inférieure ou égale à huit jours, les destructions, dégradations ou détériorations volontaires d'un bien appartenant à autrui dont il n'est résulté qu'un dommage léger ou certaines atteintes à l'état civil.

de la mort ou d'une disparition, toute personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait participé, comme auteure ou complice, à la commission de l'une de ces infractions.

La durée de conservation des données varie en fonction des individus concernés et s'établit à :

— vingt ans pour les individus majeurs mis en cause dans une affaire pénale, sous réserve des infractions pour lesquelles cette durée est réduite à cinq ans ou portée à quarante ans ;

— cinq ans pour les mineurs, sous réserve des infractions pour lesquelles elle est augmentée à dix ou vingt ans ;

— quinze ans pour les victimes d'infractions.

Les données concernant les personnes faisant l'objet d'une enquête ou instruction pour recherche des causes de la mort ou d'une disparition doivent être effacées dès lors que l'enquête a permis de retrouver la personne disparue ou d'écarter toute suspicion de crime ou délit (article R. 40-27 du même code).

Deux mécanismes d'effacement anticipé des données concernant les personnes mises en cause sont prévus par l'**article 230-8** :

— un **effacement de principe en cas de décision définitive de relaxe ou d'acquittement** ; toutefois, le procureur de la République peut en prescrire le maintien « *pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé* », auquel cas la personne en est avisée et une mention est portée dans le fichier, interdisant l'accès aux données dans le cadre d'enquêtes administratives ;

— une **possibilité d'effacement en cas de décision de non-lieu ou de classement sans suite** : en cas de maintien, justifié pour les mêmes raisons que celles précédemment évoquées, les décisions de non-lieu ou de classement sans suite font l'objet d'une mention, interdisant également l'accès aux données dans le cadre d'enquêtes administratives.

Le TAJ est placé sous le contrôle, d'une part, du procureur de la République territorialement compétent, d'autre part, d'un magistrat « référent ». Ces deux magistrats sont dotés des mêmes pouvoirs d'effacement, de rectification ou de maintien des données, la rectification étant de droit en cas de requalification judiciaire. Leurs décisions sont susceptibles de recours, devant le président de la chambre de l'instruction dans le premier cas, devant le président de la chambre de l'instruction de la cour d'appel de Paris dans le second cas (articles 230-8 et 230-9).

Le dispositif adopté par le législateur en 2011 différait quelque peu de celui-ci. En particulier, il n'autorisait l'effacement des données du TAJ en cas de classement sans suite que lorsque ce classement était motivé par une insuffisance

de charges. Il ne précisait pas les motifs conduisant au maintien de certaines données dans le fichier. Enfin, il n'offrait pas la possibilité de former un recours contre la décision du procureur de la République ou du magistrat « référent » tendant au maintien ou à l'effacement des données.

Ce dispositif avait été jugé dans son ensemble conforme à la Constitution par le Conseil constitutionnel lors de l'examen de la loi dite « LOPPSI 2 » [(1)].

La France s'est toutefois vue condamnée en 2014 par la Cour européenne des droits de l'homme. Dans son **arrêt *Brunet c. France* du 18 septembre 2014**, la Cour a jugé contraire à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales la législation française qui, à l'époque, empêchait l'effacement des données du STIC en cas de classement sans suite pour un motif autre que l'insuffisance de charges [(2)].

Cet arrêt a conduit le législateur à compléter, en 2016 [(3)], le dispositif d'effacement de certaines données du TAJ, en prévoyant :

— que l'ensemble des décisions de classement sans suite, quel qu'en soit le motif, pourrait donner lieu à effacement ;

— que les décisions du procureur de la République tendant au maintien ou à l'effacement des données devraient être prises en fonction des finalités du fichier appréciées au regard de la nature et des circonstances de commission de l'infraction et de la personnalité de leur auteur ;

— un recours contre les décisions du procureur de la République et du magistrat « référent », sur le modèle de celui prévu pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG).

La Commission nationale de l'informatique et des libertés estimait, en février 2015, à 9,5 millions le nombre d'individus figurant au TAJ au seul titre des personnes mises en cause.

2. La décision n° 2017-670 QPC du 27 octobre 2017

Saisie de la conformité à la Constitution de l'article 230-8 précité par la voie d'une question prioritaire de constitutionnalité [(4)], le Conseil constitutionnel a jugé qu'« *en privant les personnes mises en cause dans une procédure pénale,*

(1) Décision n° 2011-625 DC du 10 mars 2011, Loi d'orientation et de programmation pour la performance de la sécurité intérieure, *cons. 12 et 13.*

(2) CEDH, 18 septembre 2014, Brunet c. France*, n° 21010/10.*

(3) Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

(4) La possibilité pour le Conseil constitutionnel de statuer de nouveau sur la constitutionnalité de cette disposition, déjà déclarée conforme à la Constitution en 2011, résulte d'un changement de circonstances, le premier alinéa de l'article 230-8 précité ayant été modifié par la loi du 3 juin 2016.

autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées portent une ***atteinte disproportionnée au droit au respect de la vie privée*** » [(1)]. Il a censuré, en conséquence, le premier alinéa de l'article 230-8 précité, en reportant toutefois les effets de cette abrogation au 1er mai 2018.

Dans son analyse de proportionnalité, le Conseil constitutionnel a pris en considération le champ et la nature des données susceptibles d'être inscrites au TAJ, certaines d'entre elles étant particulièrement sensibles, le nombre important de personnes susceptibles de figurer dans ce fichier, l'absence dans la loi de durée maximum de conservation des informations enregistrées et le fait que ces informations pouvaient être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative [(2)].

3. Le dispositif proposé

a. Le projet de loi initial

Le **1° du I** du présent article propose une nouvelle rédaction du **premier alinéa de l'article 230-8**, qui apporte des garanties en matière d'effacement des données inscrites au TAJ avant la fin de la durée normale de conservation.

En premier lieu, le **contrôle opéré par le procureur de la République** territorialement compétent sur le traitement sera ***« d'office ou à la demande de la personne concernée »***, précision qui ne figurait jusqu'alors que dans les dispositions relatives au contrôle du magistrat « référent ».

En deuxième lieu, les verrous s'opposant à la possibilité de solliciter l'effacement des données pour les personnes mises en causes autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite sont levés :

— toute personne pourra désormais former, **sans délai**, une **demande d'effacement, de complément ou de rectification** des données la concernant non seulement en cas de relaxe, d'acquittement, de non-lieu ou de classement sans

---

(1) Décision n° 2017-670 QPC du 27 octobre 2017, M. Mikhail P. [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires]*, § 14.*

(2) Le commentaire aux Cahiers de cette décision relève que si elle « n'a pas (…) reconnu un "droit à l'effacement", puisqu'il reviendra à l'autorité judiciaire d'apprécier le bien-fondé de cette demande, selon des critères définis par le législateur, cette décision illustre le renforcement de la jurisprudence du Conseil constitutionnel en matière de protection de la vie privée *» et du contrôle qu'il opère sur les traitements de données personnelles, en raison notamment de «* la sensibilité renforcée, compte tenu des évolutions technologiques, des données pouvant être inscrites dans ces fichiers et le nombre croissant de personnes qui y figurent *» (pp. 19-20).*

suite mais aussi « *à la suite d'une* ***décision*** *devenue définitive (...)* ***de condamnation avec dispense de peine ou dispense de mention au casier judiciaire*** » ;

— toute personne pourra également former une **demande d'effacement, de complément ou de rectification** des données la concernant à la suite de **toute autre décision définitive de condamnation, à condition toutefois d'attendre que « *ne figure plus aucune mention dans le bulletin n° 2 de son casier judiciaire* »**.

La disparition de la mention du B2 correspond au moment où la condamnation a été considérée comme non avenue ou à celui de la réhabilitation de la personne en application des 4° et 5° de l'article 775 du code de procédure pénale. Les délais de recevabilité des demandes d'effacement varieront donc en fonction de la nature des faits ayant justifié la condamnation et du *quantum* de la peine prononcée.

En dernier lieu, l'augmentation du nombre de demandes susceptibles d'être formées conduit à porter le délai de leur examen par le procureur de la République d'un à deux mois.

Le **2° du I** tire les conséquences de cette nouvelle rédaction au troisième alinéa du même article.

Le **II** prévoit l'application de ces dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, conformément au principe de spécialité législative en vertu duquel les lois et règlements ne sont applicables aux collectivités soumises à ce principe que sur mention expresse du texte.

b. La position de la Commission

Sur proposition de votre rapporteure, la Commission a aligné, à l'article 230-9 du code de procédure pénale, le délai laissé au magistrat « référent » pour statuer sur les demandes d'effacement qui lui sont soumises sur celui prévu par le présent article pour le procureur de la République, c'est-à-dire deux mois.

DÉLAIS DE LA RECEVABILITÉ DES DEMANDES D'EFFACEMENT DE DONNÉES INSCRITES AU TAJ PAR UNE PERSONNE DÉFINITIVEMENT CONDAMNÉE
(HORS DISPENSE D'INSCRIPTION AU BULLETIN N° 2 ET DEMANDES DE RÉHABILITATION)

<table>
<tr><th>PERSONNES</th><th>Types de sanctions</th><th>Délais de recevabilité des requêtes en effacement</th><th>Point de départ des délais</th></tr>
<tr><td>MINEURS</td><td>Toutes condamnations</td><td rowspan="4">Immédiatement [1]</td><td rowspan="4">À compter du caractère définitif de la condamnation</td></tr>
<tr><td rowspan="11">MAJEURS</td><td>Contraventions</td></tr>
<tr><td>Compositions pénales</td></tr>
<tr><td>Dispenses de peines</td></tr>
<tr><td>Amendes (hors contraventions)</td><td>3 ans</td><td>À compter du paiement</td></tr>
<tr><td>Jours-amende</td><td>3 ans</td><td rowspan="2">À compter du caractère définitif de la condamnation</td></tr>
<tr><td>Peines alternatives hors jours-amende (sauf si la durée de la peine alternative est supérieure à 5 ans, auquel cas elle est maintenue au bulletin n° 2 durant toute la durée)</td><td>5 ans</td></tr>
<tr><td>Emprisonnement avec quantum réhabilitable ≤ 1 an</td><td>5 ans [2]</td><td rowspan="3">À compter de l'exécution ou de la prescription de la peine</td></tr>
<tr><td>Emprisonnement avec quantum réhabilitable ≤ 10 ans</td><td>10 ans [2]</td></tr>
<tr><td>Emprisonnement avec quantum réhabilitable dans le cas de peines multiples ≤ 5 ans</td><td>10 ans [2]</td></tr>
<tr><td>Emprisonnement non réhabilitable de plein droit (réclusion criminelle ou emprisonnement avec un quantum non réhabilitable)</td><td>40 ans [3]</td><td>À compter du caractère définitif de la condamnation</td></tr>
<tr><td>Peines avec sursis</td><td colspan="2">Lorsqu'elles sont considérées comme non avenues [4]</td></tr>
<tr><td>Suivis socio-judiciaire
Interdictions d'exercer une activité professionnelle ou bénévole impliquant un contact habituel avec des mineurs (prononcés à titre de peines complémentaires)</td><td colspan="2">À l'issue de l'expiration de ces mesures, même si la peine principale est non avenue</td></tr>
<tr><td>Suivis socio-judiciaire
Interdictions d'exercer une activité en lien avec des mineurs ; interdictions, incapacités et déchéances définitives ; peines complémentaires d'inéligibilité persistant jusqu'en fin de mesure ou d'interdiction (prononcés à titre de peine alternatives)</td><td>5 ans</td><td rowspan="2">À compter du caractère définitif de la condamnation</td></tr>
<tr><td>Déclarations d'irresponsabilité pénale pour trouble mental (seule)</td><td>Immédiatement [1]</td></tr>
<tr><td>Déclarations d'irresponsabilité pénale pour trouble mental (assortie d'une hospitalisation d'office ou d'une ou de plusieurs mesures d'interdiction visées à l'article 706-136 du CPP)</td><td colspan="2">À l'expiration de la durée de l'hospitalisation d'office ou de la mesure d'interdiction dont elle est assortie</td></tr>
</table>

[1] Ces décisions ne sont en effet pas inscrites au bulletin n° 2 du casier judiciaire.

[2] Ces délais sont doublés en cas de récidive légale.

[3] Lorsque les peines n'ont pas été suivies d'une nouvelle condamnation à une peine criminelle ou correctionnelle.

[4] C'est-à-dire si le condamné ne commet pas de nouvelle infraction dans un certain délai.

*
* *

*La Commission **adopte** successivement les amendements rédactionnels CL202, CL203 et CL205, l'amendement de cohérence CL225 et l'amendement CL206 tendant à corriger une erreur de référence, tous de la rapporteure.*

*Puis la Commission **adopte** l'article 23 **modifié**.*

Article 23 bis (nouveau)
(art. L. 1461-7 du code de la santé publique)
Coordination

A l'initiative de votre rapporteure, la Commission a adopté le présent article additionnel afin de procéder à une coordination nécessaire au 6° de l'article L. 1461‑7 du code de la santé publique afin de maintenir la possibilité pour toute personne qui en fait la demande que ses données de santé à caractère personnel ne soient pas mises à la disposition du système national des données de santé.

*
* *

*La Commission **adopte** l'amendement de coordination CL238 de la rapporteure. L'article 23* bis *est ainsi rédigé.*

Article 24
Dispositions d'entrée en vigueur

Dispositions européennes :

Article 99 du règlement (UE) 2016/679 et articles 63 et 64 de la directive (UE) 2016/680.

Résumé du dispositif et effets principaux :

Le présent article fixe la date d'entrée en vigueur des dispositions du I à III de la présente loi au 25 mai 2018. Il permet cependant, pour les traitements relevant de la directive, conformément à l'article 63 de celle-ci, un report de l'obligation de journalisation au 6 mai 2023 ou au 6 mai 2026 au plus tard, dans certaines circonstances.

Modifications adoptées par la commission des Lois :

Sur proposition de votre rapporteure, la Commission a adopté un amendement de clarification rédactionnelle.

Le présent article précise la date d'entrée en vigueur des dispositions des titres I à III de la présente loi qui procèdent à la transposition du règlement (UE) 2016/679 et de la directive (UE) 2016/680.

1. L'entrée en application du règlement général sur la protection des données

L'article 99 du règlement (UE) 2016/679 précise que le règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*, soit le 25 mai 2016. Il est directement applicable à partir du 25 mai 2018 dans tout État membre. Il est obligatoire dans tous ses éléments.

Le considérant 171 du règlement précise que la directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement doivent être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable de traitement puisse le poursuivre après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.

2. La date de transposition de la directive relative aux traitements en matière pénale

L'article 64 de la directive (UE) 2016/680 précise qu'elle entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*, soit le 5 mai 2016.

L'article 63 de la directive prévoit également les règles de transposition applicables aux États membres de la manière suivante.

Les États membres adoptent et publient, au plus tard le 6 mai 2018, les dispositions législatives, règlementaires et administratives nécessaires pour se conformer à la directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions. Ils appliquent ces dispositions à partir du 6 mai 2018.

Il s'ensuit un décalage de 19 jours avec les dispositions d'entrée en vigueur du règlement dans l'ensemble des États membres.

En outre, deux dérogations sont envisagées par la directive afin de permettre un report de l'obligation de journalisation mentionnée à l'article 25, paragraphe 1, qui impose aux États membres de prévoir que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la

communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales. Le responsable de traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle, sur demande.

Ces deux dérogations sont les suivantes :

— un État membre peut prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant le 6 mai 2016 sont mis en conformité avec l'article 25, paragraphe 1, de la directive au plus tard le 6 mai 2023 ;

— un État membre peut, dans des circonstances exceptionnelles, mettre un système donné de traitement automatisé en conformité avec l'article 25, paragraphe 1, dans un délai déterminé après le 6 mai 2023, lorsque, à défaut de cela, de graves difficultés se poseraient pour le fonctionnement du système de traitement automatisé en question. L'État membre concerné notifie à la Commission les raisons de ces graves difficultés et les motifs justifiant le délai déterminé de mise en conformité du système donné de traitement automatisé avec l'article 25, paragraphe 1. Le délai déterminé n'est en aucun cas fixé au-delà du 6 mai 2026.

3. L'entrée en vigueur de la présente loi

Malgré le décalage de 19 jours entre l'entrée en vigueur de la directive (6 mai 2018) et celle du règlement (25 mai 2018), le premier alinéa du présent article prévoit, dans une optique de sécurité juridique et de simplification, une entrée en vigueur indifférenciée pour les titres I^{er} à III de la présente loi, le 25 mai 2018.

Toutefois, conformément aux dérogations prévues par la directive s'agissant de l'obligation de journalisation mentionnée à l'article 25, paragraphe 1, le deuxième alinéa du présent article précise que les dispositions de l'article 70-15 de la loi n° 78-17 du 6 janvier 1978 résultant de l'article 19 du présent projet de loi et relatives à cette obligation de journalisation, pourront entrer en vigueur à une date ultérieure ne pouvant excéder le 6 mai 2023 lorsqu'une telle obligation exigerait des efforts disproportionnés, et ne pouvant excéder le 6 mai 2026, lorsque, à défaut d'un tel report, il en résulterait de graves difficultés pour le fonctionnement du système de traitement automatisé. La liste des traitements concernés par ces reports et les dates auxquelles, pour ces traitements, l'entrée en

vigueur de cette obligation sera reportée seront déterminées par voie règlementaire.

*
* *

La Commission ***adopte*** *l'amendement rédactionnel CL217 de la rapporteure.*

Elle ***adopte*** *ensuite l'article 24* ***modifié****.*

Après l'article 24

La Commission examine l'amendement CL44 de Mme Danièle Obono.

Mme Danièle Obono. Il semble exister un consensus national, transpartisan, pour préserver et renforcer la neutralité du Net, qui est essentielle. Nous nous en félicitons et nous souhaitons contribuer, comme nous l'avons fait tout au long de l'examen du projet de loi, n'en déplaise à certains, à élargir et à structurer encore mieux les débats en la matière.

Notre amendement vise à retranscrire le consensus actuel en précisant la définition juridique de la neutralité du Net. Nous reprenons des amendements déposés sous la précédente législature, et qui étaient notamment cosignés par le président de Rugy. Dans ces conditions, je ne doute pas que vous soyez en faveur de notre proposition.

Mme la rapporteure. Je suis d'accord sur le fond. J'ai même proposé, dans le cadre des groupes de travail sur la réforme de l'Assemblée, que ce principe soit inscrit dans la Constitution. Il me semble que le projet de loi n'est pas le bon véhicule juridique : les débats constitutionnels à venir permettront d'élever votre proposition au plus haut niveau dans notre ordre juridique. Je donne donc un avis défavorable.

La Commission ***rejette*** *l'amendement.*

Puis elle ***adopte*** *l'ensemble du projet de loi* ***modifié****.*

*
* *

En conséquence, la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République vous demande ***d'adopter*** *le projet de loi (n° 490) relatif à la protection des données personnelles dans le texte figurant dans le document annexé au présent rapport.*

ANNEXE : LES FORMALITÉS PRÉALABLES À LA MISE EN ŒUVRE D'UN TRAITEMENT AVANT ET APRÈS LA RÉFORME

<table>
<tr><th>Traitements de données à caractère personnel
(hors traitements de données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques)</th><th>Formalités avant la réforme</th><th>Formalités après la réforme</th></tr>
<tr><td colspan="3">Traitements de données non sensibles</td></tr>
<tr><td>Traitements de droit commun</td><td>Déclaration auprès de la CNIL</td><td rowspan="5">Analyse d'impact préalable en cas de risque élevé pour les droits et libertés des personnes et, le cas échéant, consultation de la CNIL</td></tr>
<tr><td>Traitements ayant pour seul objet la tenue d'un registre exclusivement destiné à l'information du public</td><td rowspan="2">Pas de formalité préalable</td></tr>
<tr><td>Certains traitements mis en œuvre par une association ou un organisme à but non lucratif à caractère religieux, philosophique, politique ou syndical</td></tr>
<tr><td>Traitements pour lesquels le responsable a désigné un correspondant à la protection des données, sans transfert des données à un pays non membre de l'UE</td><td>Pas de formalité préalable</td></tr>
<tr><td>Traitements de données de santé mis en œuvre par les organismes ou services chargés d'une mission de service public en vue de répondre, en situation d'urgence, à une alerte sanitaire</td><td>Déclaration auprès de la CNIL</td></tr>
<tr><td colspan="3">Traitements de données sensibles ou mis en œuvre par l'État ou pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public</td></tr>
<tr><td>Traitements statistiques mis en œuvre par l'INSEE et les services statistiques ministériels</td><td rowspan="8">Autorisation par la CNIL</td><td rowspan="8">Analyse d'impact préalable en cas de risque élevé pour les droits et libertés des personnes et, le cas échéant, consultation de la CNIL</td></tr>
<tr><td>Traitements de données qui font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci (*) et qui font l'objet, à bref délai, d'un procédé d'anonymisation ou sont justifiés par l'intérêt public</td></tr>
<tr><td>Traitements portant sur des données génétiques, sauf ceux mis en œuvre par des médecins ou biologistes aux fins de médecine préventive, de diagnostics médicaux ou d'administration de soins ou de traitements</td></tr>
<tr><td>Traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux mis en œuvre par des auxiliaires de justice aux fins de défense des personnes</td></tr>
<tr><td>Traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de disposition législative ou réglementaire</td></tr>
<tr><td>Traitements ayant pour objet l'interconnexion de fichiers relevant de personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ou d'autres personnes et dont les finalités sont différentes</td></tr>
<tr><td>Traitements comportant des appréciations sur les difficultés sociales des personnes</td></tr>
<tr><td>Traitements mis en œuvre par toute personne autre que l'État comportant des données biométriques nécessaires au contrôle de l'identité des personnes</td></tr>
</table>

<table>
<tr><td>Traitements mis en œuvre pour le compte de l'État qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté</td><td>Autorisation par arrêté du ou des ministres compétents, pris après avis motivé et publié de la CNIL (**)</td><td rowspan="2">Analyse d'impact préalable en cas de risque élevé pour les droits et libertés des personnes et, le cas échéant, consultation de la CNIL</td></tr>
<tr><td>Mêmes traitements lorsqu'ils font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci (*)</td><td>Autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL (**)</td></tr>
<tr><td>Traitements de données mis en œuvre pour le compte de l'État portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes</td><td colspan="2">Autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>Mêmes traitements de données mais portant sur des données génétiques</td><td>Autorisation par la loi ou la CNIL</td><td>Autorisation par la loi ou par décret en Conseil d'État pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>Traitements mis en œuvre pour le compte de l'État portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes :
– qui ne comportent aucune donnée faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci (*) ;
– qui ne comportent aucune donnée relative aux infractions, condamnations et mesures de sûreté ;
– qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;
– et qui sont mis en œuvre par des services ayant pour mission de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés ou d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, ou d'établir des statistiques</td><td rowspan="2">Autorisation par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant, pris après avis motivé et publié de la CNIL</td><td rowspan="2">Analyse d'impact préalable en cas de risque élevé pour les droits et libertés des personnes et, le cas échéant, consultation de la CNIL</td></tr>
<tr><td>Traitements relatifs au recensement de la population</td></tr>
</table>

(*) La réforme ajoute à cette liste des données sensibles les données biométriques, génétiques et celles relatives à l'orientation sexuelle.

(**) Un décret en Conseil d'État peut dispenser de publication l'acte d'autorisation : seul le sens de l'avis de la CNIL est alors publié, en même temps que le décret autorisant la dispense de publication de l'acte.

<table>
<tr><th>Traitements de données à caractère personnel impliquant le NIR ou la consultation du RNIPP</th><th>Formalités avant la réforme</th><th>Formalités après la réforme</th></tr>
<tr><td>Traitements comportant le NIR parmi les données traitées mis en œuvre pour le compte ou par…</td><td></td><td></td></tr>
<tr><td>… une personne privée</td><td>Autorisation par la CNIL</td><td rowspan="2">Autorisation par « décret-cadre » en Conseil d’État, pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>… l’État, une personne morale de droit public ou une personne morale de droit privé mettant en œuvre un service public ou le service statistique public</td><td>Autorisation par décret en Conseil d’État pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>Traitements impliquant la consultation du RNIPP mis en œuvre pour le compte ou par…</td><td></td><td></td></tr>
<tr><td>… une personne privée</td><td>Autorisation par la CNIL</td><td rowspan="4">Autorisation par « décret-cadre » en Conseil d’État, pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>… l’État, une personne morale de droit public ou une personne morale de droit privé mettant en œuvre un service public ou le service statistique public</td><td>Autorisation par arrêté ou décision de l’organe délibérant, après avis motivé et publié de la CNIL</td></tr>
<tr><td>Traitements du NIR à des fins de recherche médicale</td><td>Autorisation par la CNIL après avis d’un comité d’expertise</td></tr>
<tr><td>Traitements de données de santé utilisant le NIR, mis en œuvre par des organismes ou services chargés d’une mission de service public afin de répondre, en cas d’urgence, à une alerte sanitaire</td><td>Déclaration auprès de la CNIL dans un cadre défini par décret en Conseil d’État</td></tr>
<tr><td>Traitements du NIR à des fins de veille sanitaire ou de gestion des services sanitaires et médico-sociaux</td><td colspan="2">Autorisation par la loi
(art. L. 1111-8-1 du code de la santé publique)</td></tr>
<tr><td>Traitements du NIR pour l’offre de téléservices aux usagers de l’administration</td><td>Autorisation par arrêté ou décision de l’organe délibérant, après avis motivé et publié de la CNIL</td><td>Autorisation par « décret-cadre » en Conseil d’État, pris après avis motivé et publié de la CNIL, sans garanties de cryptage</td></tr>
<tr><td>Traitements du NIR à des fins de statistique publique par l’INSEE (droit commun)</td><td>Déclaration auprès de la CNIL avec garanties de cryptage</td><td rowspan="3">Autorisation par « décret-cadre » en Conseil d’État, pris après avis motivé et publié de la CNIL, avec garanties de cryptage</td></tr>
<tr><td>Traitements du NIR à des fins de statistique publique par l’INSEE (les données traitées sont des données faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l’appartenance syndicale des personnes, ou relatives à la santé ou à la vie sexuelle de celles-ci ^(*) ou des données relatives aux infractions, condamnations et mesures de sûreté)</td><td>Autorisation par décret en Conseil d’État pris après avis motivé et publié de la CNIL</td></tr>
<tr><td>Traitements du NIR à des fins de recherche scientifique ou historique</td><td>Autorisation par la CNIL avec garanties de cryptage</td></tr>
</table>

(*) La réforme ajoute à cette liste des données sensibles les données biométriques, génétiques et celles relatives à l’orientation sexuelle.

CONTRIBUTION DE M. PHILIPPE GOSSELIN, CO-RAPPORTEUR SUR LA MISE EN APPLICATION DE LA LOI
(article 86, alinéa 7, du Règlement)

La protection de la vie privée et des données personnelles de nos concitoyens représente, depuis de longues années déjà, un enjeu majeur des politiques publiques dans notre pays. L'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés et la création de la Commission nationale de l'informatique et des libertés (CNIL) ont fait de la France l'un des premiers pays au monde à se doter d'une législation et d'une autorité de contrôle indépendante sur ces questions.

Certes, nous ne sommes plus dans le contexte des années 1974 où les fichiers du système SAFARI défrayaient la chronique et avaient, fort habilement, permis de créer les premières autorités administratives indépendantes, appelées à former ce qui était alors présenté comme le « carré magique » de la transparence : la Commission des opérations de bourse, le Médiateur, la Commission d'accès aux documents administratifs et la CNIL.

Mais, en cette période du 40e anniversaire de la CNIL, que nous avons célébré dignement, et comme il se devait, le jeudi 25 janvier, il est important de s'inscrire dans l'héritage de cette période créatrice où le souci de protection des libertés était déjà, évidemment, un objectif essentiel.

Fort de son expérience dans ces domaines de la protection de la vie privée et des données personnelles, notre pays a toujours été l'un des États les plus impliqués sur ces thématiques, aussi bien au sein de l'Union européenne que sur la scène internationale.

Les principes de la loi du 6 janvier 1978 ont, pour une grande part, fortement inspiré les dispositions de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dont l'adoption, en 1995, a constitué l'acte fondateur de la politique européenne dans ce domaine.

L'explosion d'internet, l'émergence des réseaux sociaux, l'apparition de nouvelles technologies et de nouvelles pratiques ont considérablement, c'est peu que de le dire, transformé le monde numérique, digital, depuis l'adoption de la directive en 1995.

Les données personnelles des citoyens ne sont plus seulement, et bien loin s'en faut, contenues dans des fichiers mis en place par les États ou les administrations comme cela était souvent le cas à l'origine. Elles sont désormais bien traitées par différents acteurs publics, et très largement privés, dont la croissance est exponentielle à l'heure des *datas*, des *open datas* et autres ouvertures des données, qui sont sans doute, et à juste titre, présentées comme LA matière première du XXIe siècle.

À cette nouvelle réalité s'ajoute, fort logiquement et conséquemment, une internationalisation croissante, elle aussi exponentielle, des échanges de données : les traitements de données sont totalement mondialisés, s'affranchissent des frontières traditionnelles, sans que les citoyens en soient nécessairement informés, sans, en tout cas, qu'ils s'en rendent réellement compte, et qu'ils intègrent profondément cet élément, et sans qu'ils puissent, véritablement, en conserver la maîtrise.

C'est dans ce contexte, en forte évolution pour ne pas dire révolution, que la Commission européenne faisait de la révision du cadre juridique européen une priorité stratégique de son action avec pour objectif premier l'harmonisation et la simplification des règles applicables en Europe.

Le processus est ancien.

Ainsi, dès 2009, une consultation publique de l'ensemble des acteurs du secteur était publiée qui, d'une certaine façon, donnait le top départ.

Mais les années ont passé.

Les résultats se sont un peu fait attendre. Nous nous en étions émus à l'Assemblée nationale et, sur ma proposition, en février 2012, une motion européenne avait été adoptée par la Délégation aux Affaires européennes, qui revenait sur la nécessaire réforme de la directive, et les propositions que nous formulions.

Je dois aussi, du reste, saluer la CNIL qui a joué un grand rôle dans le déroulement des travaux préparatoires, saluer l'action d'Alex TURK, président de cette autorité, au début des travaux, celle qui lui a succédé, Isabelle FALQUE-PIERROTIN, et de l'ensemble du groupe G 29, le groupe des « Cnil », c'est à dire des autorités de contrôle (ce sera mieux dit !) européennes.

Après plusieurs années de négociations, l'adoption du règlement général sur la protection des données le 27 avril 2016 a constitué l'aboutissement de la volonté européenne.

Le règlement a été complété par une directive sur les données policières et judiciaires, ces deux textes constituant désormais « le paquet » données personnelles.

Le règlement du 27 avril 2016 sera applicable à compter du 25 mai 2018, date à laquelle la directive 95/46 sera abrogée.

Il est donc nécessaire d'adapter préalablement le cadre législatif de la protection des données à caractère personnel.

Si la loi du 7 octobre 2016 pour une République numérique a bien permis un renforcement significatif de la protection des données personnelles, elle n'a cependant pas couvert l'ensemble du champ du règlement et la révision de la loi de 1978 est indispensable.

C'est bien l'objet du présent texte.

Je salue la qualité du travail de notre rapporteure Paula FORTEZA.

Je regrette cependant la précipitation avec laquelle ces travaux sont menés et l'habilitation donnée au Gouvernement pour agir et transcrire directement la directive par ordonnance.

Contrairement à ce qu'a dit la garde des Sceaux en commission des Lois, il ne s'agit pas, avec cette transposition, de simples ajustements légistiques de mise en conformité de la loi de 1978.

Bien consciente que cela pouvait hélas se dérouler ainsi, la précédente commission des Lois nous avait chargés, Anne-Yvonne Le Dain et moi-même, d'un rapport d'information sur « *les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française* ».

Il y avait là un passage de relais qui expliquait les enjeux et proposait un calendrier.

Hélas, c'est comme si nous n'avions rien fait, la précipitation est bien de mise et cela nuit, pour une part, à la qualité de notre législation.

La fabrique de la loi ne devrait pouvoir se faire dans une telle précipitation. C'est un message envoyé, aussi, à chacun, à l'heure où l'Assemblée nationale va se pencher sur des propositions de nouveaux calendriers, de nouvelles méthodes de travail législatif.

Quoi qu'il en soit, ce texte est d'une très grande importance et marque un profond changement de paradigme.

L'espace disponible pour la contribution ne permet pas de détailler, ici, l'ensemble des apports du nouveau règlement et de la directive qui lui est associée.

Les thèmes et notions développés y sont extrêmement importants : la portabilité, le déréférencement, l'anonymisation, le consentement, le profilage, la réparation, la responsabilité, la sous-traitance la notion de prévention, celle d'impact, celle de risque élevé, la nécessité d'informer les autorités de référence dans un délai court, le concept de dialogue et celui d'obligation faite aux entreprises de prévoir le risque… Toutes ces notions comportent une marge d'interprétation importante. Il est donc essentiel que la France construise autour de ces éléments un dispositif qui serve à la fois son économie et l'intérêt de ses citoyens.

Retenons que la loi de 1978 nous avait habitués, si l'on schématise et simplifie un peu, à une forme de « confort », à la fois pour les particuliers et pour les entreprises, sous la forme d'un système de déclarations préalables et d'autorisations. Demain, la charge de la preuve sera totalement inversée : il reviendra aux entreprises de démontrer qu'elles ont pris toutes les précautions nécessaires pour garantir le respect des données personnelles. Pensons, à ce propos, à bien les accompagner dans cette nouvelle approche.

C’est le principe de responsabilité qui est mis en œuvre avec comme contrepartie des sanctions beaucoup plus fortes : jusqu’à 4 % du chiffre d’affaire annuel consolidé, et jusqu’à 20 millions d’euros. Bien loin des 150 000 euros maximum que la CNIL, par exemple, en France peut actuellement prononcer dans le cadre des sanctions.

Tout cela n’est pas simple à mettre en œuvre. Il va falloir, sans aucun doute, être capable de « disrupter » !

La question de la protection des données personnelles des particuliers suscite aussi le débat : nous avons notamment soulevé le cas des mineurs, dont le consentement demeure un point important. Je constate d’ailleurs que le débat n’est pas clos entre les commissaires et la majorité : le Gouvernement défendait l’âge de seize ans en se calant sur le règlement européen tandis que la rapporteure proposait l’âge de quinze ans, comme je le faisais moi-même par amendement, par cohérence avec d’autres textes, notamment ceux relatifs à la « majorité sexuelle ». Un autre amendement de la majorité, qui sera peut-être redéposé en séance, proposait de le fixer à treize ans.

Nous verrons ce que donnera le débat, qui traverse aussi la société car les parents, les jeunes et les adolescents peuvent avoir des points de vue différents. Il est bon que ce débat puisse se poursuivre.

De même, au-delà des pouvoirs de la CNIL qu’il faut adapter, sur les lignes directrices qu’elle pourrait émettre, ou pas, sur ce droit souple qui lui serait reconnu, ou pas, il faut saisir l’occasion de ces textes pour renforcer les droits de nos concitoyens, affirmer la protection des mineurs et de nouveaux droits (comme l’action de groupe) dans la continuité et la complémentarité de ceux avancés dans la loi pour une République numérique, dite « loi Lemaire », promulguée en 2016. Les débats d’alors avaient régulièrement renvoyé à l’adaptation du règlement européen et de la directive, mais nous étions restés souvent en deçà de ces textes pour des raisons qualifiées de pragmatique, mais aussi, il faut le reconnaître, parfois, assez politiques.

En conclusion :

Au-delà de l’adoption du texte, qui ne fait pas de doute, la prise en compte des données personnelles doit se poursuivre. C’est un droit fondamental, incontournable.

Préservons la singularité de la protection des données en France, qui est affirmée et réaffirmée avec force et conviction, notamment, par la CNIL. Saluons cette institution qui, ces dernières années, a su prendre une place très particulière en Europe en matière de protection des données, et qui permet sans doute de promouvoir, à juste titre, un modèle français, voire européen, auquel nous sommes attachés. Il doit exclure toute marchandisation poussée à l’extrême et réaffirmer la protection des données, en général, et de certaines données particulières, comme les données de santé.

Dans un monde en éternelle concurrence, où les modèles du droit continental et du droit anglo-saxon s'affrontent, saluons l'adoption d'un règlement et d'un ensemble de textes européens, adaptés en droit français, ambitieux.

L'Europe, souvent si décriée et caricaturée, affiche ainsi sa capacité d'adaptation aux enjeux de la mondialisation, tout en respectant un solide héritage humaniste.

Cela deviendra, au-delà des obligations légales et réglementaires, une référence incontournable, et peut-être, souhaitons-le, un avantage concurrentiel dans ce monde, plus souvent qu'on ne le pense, en recherche de sens.

LISTE DES PERSONNES ENTENDUES PAR LA RAPPORTEURE

ADMINISTRATIONS

- **Assistance publique – Hôpitaux de Paris – Délégation à la recherche clinique et à l'innovation**
  - Mme Lauren Demerville, responsable du pôle Partenariats et expertises
- **Direction interministérielle du numérique et du système d'information et de communication de l'État**
  - M. Henri Verdier, directeur
  - M. Perica Sucevic, chef du pôle juridique, adjoint à la cheffe de la mission Étalab
  - M. Thomas Menant, chargé de mission
  - Mme Maud Choquet, chargée de mission
- **Ministère des Armées**
  - Mme Claire Legras, directrice des affaires juridiques
  - M. Mathieu Rhée, conseiller à la direction des affaires juridiques
  - M. Christophe Junqua, conseiller du cabinet militaire de la ministre
  - Mme Animya N'Tchandy, conseillère parlementaire au cabinet de la ministre
- **Ministère de l'Économie, des finances, de l'action et des comptes publics – Institut national de la statistique et des études économiques**
  - M. Jean-Luc Tavernier, directeur général
  - M. Patrick Redor, chef de l'unité Affaires juridiques et contentieuses
  - M. Benoît Ourliac, directeur de cabinet
- **Ministère de l'Éducation nationale – Inspection générale de l'éducation nationale**
  - M. Gilles Braun, inspecteur général de l'éducation nationale, auteur du rapport sur les données scolaires
  - M. David Knecht, conseiller numérique au cabinet du ministre
- **Ministère de l'Intérieur**
  - M. Thomas Campeaux, directeur des libertés publiques et des affaires juridiques
  - M. Eric Tison, sous-directeur des libertés publiques
  - Mme Anne-Sophie Mach, cheffe du bureau de la liberté individuelle

- **Ministère de la Santé – Délégation à la recherche clinique et à l'innovation**
  - — Mme Laurene Demerville, responsable du pôle Partenariat et expertise
  - — Mme Zouleikha Bentoumi, juriste
- **Secrétariat général des affaires européennes**
  - — Mme Sandrine Gaudin, secrétaire générale
  - — Mme Clémence Olsina, conseillère juridique auprès de la secrétaire générale
  - — Mme Constance Deler, chef du secteur Parlements
  - — M. Renaud Halem, chef du secteur Espace judiciaire européen
  - — Mme Eve Jullien, adjointe au chef du secteur Espace judiciaire européen
- **Secrétariat d'État chargé du numérique**
  - — M. Côme Berbain, conseiller chargé de la transformation numérique de l'État et de la sécurité numérique

AUTORITÉS ADMINISTRATIVES INDÉPENDANTES ET ORGANISMES PUBLICS

- **Commission nationale consultative des droits de l'homme**
  - — M. Thomas Dumortier, conseiller juridique
  - — M. Malcolm Théoleyre, conseiller pour les questions de société, d'éthique et d'éducation aux droits de l'homme
- **Commission nationale de contrôle des techniques de renseignement**
  - — M. Francis Delon, président
  - — M. Samuel Manivel, conseiller
- **Commission nationale de l'informatique et des libertés**
  - — M. Jean Lessi, secrétaire général
  - — M. Thomas Dautieu, directeur-adjoint à la direction de la conformité
  - — M. Mathias Moulin, directeur-adjoint à la direction de la protection des droits et des sanctions
  - — M. Émile Gabrié, chef du service régalien et collectivités territoriales
  - — Mme Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires
- **Conseil national du numérique**
  - — M. Jan Krewer, secrétaire général adjoint (contribution écrite)

- **Institut national des données de santé**
  - — Mme Dominique Polton, présidente
- **Institut national de recherche en informatique et en automatique**
  - — M. Daniel le Métayer, directeur de recherche

AVOCATS

- **Conseil national des barreaux** (*)
  - — Mme Christiane Féral-Schuhl, présidente
  - — Mme Laurence Dupont, juriste, adjointe à la directrice du pôle juridique, correspondante « Informatique et libertés »
  - — M. Jacques Edouard Briand, directeur des affaires législatives
  - — M^e^ Etienne Papin, avocat
- **Delsol Avocats**
  - — M^e^ Jeanne Bossi-Malafosse, avocate associée, responsable du département de la protection des données personnelles

UNIVERSITAIRES

- — Mme Judith Rochfeld, professeure des universités, membre de l'Institut de recherche juridique de la Sorbonne
- — Mme Olivia Tambou, maître de conférences spécialisée en droit du marché intérieur de l'Union européenne à l'Université Paris-Dauphine

ACTEURS ÉCONOMIQUES

- **Amazon** (contribution écrite)
- **Alan**
  - — M. Charles Gorintin, directeur de la technologie
- **Facebook** (*)
  - — M. Anton Maria Battesti, responsable des affaires publiques
  - — Mme Ophélie Gerullis, responsable des affaires publiques
  - — M. Nicolas de Bouville, directeur de la protection de la vie privée
- **Google** (*)
  - — M. Olivier Esper, directeur des relations institutionnelles
  - — M. Benjamin Amaudric du Chaffaut, avocat conseil
- **Implicity**
  - — Mme Caroline Florequin, responsable réglementaire

- **Microsoft**
  - — M. Marc Mossé, senior director EU government affairs
  - — M. Jean-Renaud Roy, corporate affairs director
- **Twitter** (*)
  - — Mme Audrey Herblin-Stoop, directrice des affaires publiques
- **Association française des entreprises privées** (contribution écrite)
- **Association des sites numériques communautaires**
  - — M. Giuseppe de Martino, président
- **Chambre de commerce internationale (CCI)**
  - — Mme Stéphanie Faber, avocate du cabinet Squire Patton Boggs, membre de la CCI
  - — Mme Lee Carter Bolton, business development, comité national français de la CCI
  - — Mme Sophie Tomlinson, assistante policy manager
- **Fédération des industries électriques, électroniques et de communication**
  - — M. Guillaume Adam, chef du service des affaires européennes et numériques
  - — Mme Julie Macaire, chef du service des affaires juridiques
  - — M. Gabriel Daubech, responsable des affaires publiques du syndicat national de l'industrie des technologies médicales
- **Mouvement des entreprises de France** (*) (contribution écrite)
- **Syndicat des régies internet**
  - — Mme Hélène Chartier, directrice générale
  - — M. Clément Reix, chargé de la politique publique chez Dailymotion (*)
  - — M. Jean-Luc Archambault, président de Lysios Public Affairs (*)
- **Syntec numérique** (*)
  - — Mme Emilie Dumérain, déléguée juridique
  - — M. Sébastien Duplan, délégué relations institutionnelles

ASSOCIATIONS

- **Association e-enfance**
  - — Mme Justine Atlan, directrice
  - — M. Samuel Comblez, psychologue-directeur des opérations
- **Association e-génération** (contribution écrite)

- **Association française des correspondants à la protection des données personnelles**
  - — M. Paul-Olivier Gibert, président
  - — Mme Pascale Gelly, vice-présidente
- **European digital rights (EDRi)**
  - — Mme Estelle Massé, analyste principale des politiques pour Access Now, membre de l'EDRi
- **Exégètes amateurs**
  - — M. Hugo Roy, membre
  - — M. Alexis Fitzjean O Cobhthaigh, membre
- **Quadrature du net**
  - — M. Arthur Messaud, juriste
- **UFC Que choisir**
  - — Mme Justine Massera, juriste spécialisée dans les nouvelles technologies
  - — M. Guilhem Fenieys, chargé de mission Relations institutionnelles
  - — M. Arthur Messaud, juriste

La commission des Lois a par ailleurs effectué un déplacement à la Commission nationale de l'informatique et des libertés le 23 novembre 2017 en vue de préparer l'examen du présent texte.

(*) Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique, s'engageant ainsi dans une démarche de transparence et de respect du code de conduite établi par le Bureau de l'Assemblée nationale.