N° 577

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 18 janvier 2018.

RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA COMMISSION DES AFFAIRES EUROPÉENNES [1]

portant observations sur le projet de loi
relatif à la **protection des données personnelles** (n° 490)

ET PRÉSENTÉ

PAR Mme Christine HENNION
Députée

(1) La composition de la commission figure au verso de la présente page.

La Commission des affaires européennes est composée de : Mme Sabine THILLAYE, *présidente* ; MM. Pieyre-Alexandre ANGLADE, Jean-Louis BOURLANGES, Bernard DEFLESSELLES, Mme Liliana TANGUY, *vice-présidents* ; Mme Sophie AUCONIE, M. André CHASSAIGNE, Mmes Marietta KARAMANLI, Danièle OBONO, *secrétaires ;* MM. Damien ABAD, Patrice ANATO, Mme Aude BONO-VANDORME, MM. Éric BOTHOREL, Vincent BRU, Mmes Fannette CHARVIER, Yolaine de COURSON, Typhanie DEGOIS, Marguerite DEPREZ-AUDEBERT, M. Benjamin DIRX, Mmes Coralie DUBOST, Françoise DUMAS, MM. Pierre-Henri DUMONT, Alexandre FRESCHI, Bruno FUCHS, Mmes Valérie GOMEZ-BASSAC, Carole GRANDJEAN, Christine HENNION, MM. Michel HERBILLON, Alexandre HOLROYD, Christophe JERRETIE, Jérôme LAMBERT, Mmes Constance Le GRIP, Nicole Le PEIH, MM. Jean-Claude LECLABART, Ludovic MENDES, Thierry MICHELS, Christophe NAEGELEN, Mme Valérie PETIT, MM. Damien PICHEREAU, Jean-Pierre PONT, Joaquim PUEYO, Didier QUENTIN, Mme Maina SAGE, MM. Raphaël SCHELLENBERGER, Benoit SIMIAN, Éric STRAUMANN, Mmes Michèle TABAROT, Alice THOUROT.

SOMMAIRE

INTRODUCTION

Mesdames, Messieurs,

Après de longues années de négociations, **l'Union européenne s'apprête à définir un cadre juridique global pour la protection des données personnelles de l'ensemble des citoyens européens**.

Le Règlement général de protection des données (RGPD) [(1)], qui doit s'appliquer au 25 mai 2018, représente un effort sans précédent, et sans doute jusque-là inégalé, de définir un standard commun en la matière.

La capacité de l'Union à légiférer en matière de protection des données personnelles tient avant tout à l'intégration de ce principe à l'article 8 de la Charte des Droits Fondamentaux, au même titre que la protection de la vie privée [(2)]. La reprise à l'article 16 du TFUE [(3)] (Traité sur le fonctionnement de l'Union européenne) des règles de protection des données personnelles découle directement de la force juridique conférée à la Charte des Droits Fondamentaux par le Traité de Lisbonne, et notamment de son article 8.

Ce texte, de portée mondiale, puisqu'il devra être appliqué par tout organisme traitant les données personnelles des résidents européens, est fondateur pour la garantie des libertés dans le monde numérisé du XXI^{e} siècle. La restauration de la confiance des utilisateurs dans le domaine du numérique aura pour conséquence directe le développement des entreprises au sein du marché unique numérique. Sans nier l'importance de l'équilibre à trouver pour assurer une mise en œuvre pratique et efficace par les entreprises et la possibilité d'innovations, l'objectif premier de ce texte est bien le droit à la vie privée des

---

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(2) 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

(3) 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

personnes. C'est donc avec ce regard que la lecture critique de ce texte doit être faite.

Ce règlement confère en effet de nouveaux droits aux individus. **Les droits déjà existants d'accès aux données et de droit à l'information sont renforcés et s'y ajoutent des droits à l'effacement (ou « droit à l'oubli ») et le droit à la portabilité des données**, susceptibles de garantir aux citoyens une maîtrise renouvelée de leurs données. Pour ce qui est des entreprises, le règlement permet d'inverser le paradigme traditionnel du régime d'autorisation. La confiance envers les responsables de traitement et leurs sous-traitants implique désormais que ce soit eux, accompagnés dans la mesure de leurs moyens par les autorités de contrôle nationales, qui vérifient la licéité de leurs traitements des données à caractère personnel. En échange de cette plus grande souplesse, le contrôle exercé désormais *a posteriori* prend de nouvelles formes.

Les autorités de contrôle nationales bénéficient en effet de la possibilité d'infliger des amendes administratives plus lourdes, allant jusqu'à 4 % du chiffre d'affaires mondial pour les violations les plus graves, mais elles peuvent aussi beaucoup plus facilement collaborer entre elles. **Les modalités de coordination des autorités nationales dans leurs enquêtes et l'assistance qu'elles offrent auprès des acteurs du numérique permettent la bonne application des dispositions du règlement à tous les traitements de données, y compris les traitements transfrontaliers**.

La **protection globale des droits fondamentaux au sein de l'Union européenne doit enfin définir un standard susceptible d'influencer la formation des normes sur les autres continents**. À ce titre, l'application extra-continentale des dispositions du règlement à des entreprises de pays tiers, et notamment américaines et chinoises, visant des personnes résidant sur le territoire européen est seule à même de garantir l'effet utile du règlement.

Le projet de loi sur lequel le présent rapport expose des observations adapte notamment la législation nationale au RGPD et transpose la directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Le RGPD, compte tenu de l'ampleur du domaine concerné, ainsi que de la longueur des négociations, a laissé un grand nombre – plus d'une cinquantaine – de marges de manœuvre aux États membres pour faire des choix dans l'application de certaines dispositions. Nous ne pouvons que le regretter, ceci affaiblissant la portée du texte. Si des points majeurs, tels que les nouveaux droits pour les personnes concernées ou la nécessité de collaborer entre les agences nationales de contrôle ne permettent pas de telles marges de manœuvre, **il n'en demeure pas moins que celles-ci sont sources de divergence réglementaire**. **Le coût sera supporté par les entreprises européennes, et les PME au premier chef**, puisqu'elles ne disposent souvent pas des capacités juridiques et

économiques pour se conformer à la fois au RGPD et à la diversité des législations nationales. Ceci est tout à fait dommageable, quand au même moment, dans leur déclaration commune pour le 22 janvier 2018, les parlements français et allemands plaident pour la réalisation d'un espace économique franco-allemand avec des règles harmonisées, notamment en ce qui concerne le droit des entreprises.

Il est donc d'autant plus appréciable que le gouvernement ait fait un choix parcimonieux et, pour la majorité d'entre elles, pertinent, de l'usage des marges de manœuvre nationales. Votre rapporteure s'est attachée à essayer de comprendre les écarts entre les marges de manœuvre nationales afin d'estimer les potentiels obstacles à leur application harmonieuse. L'ensemble des pays européens travaillant actuellement en parallèle, les informations ne sont que partiellement disponibles.

Il n'en demeure pas moins nécessaire de modifier le projet de loi dans certaines matières, **telles que le traitement des données pour le compte de l'État, l'âge de consentement des mineurs ou la possibilité de mener une action de groupe en réparation du fait de la violation des dispositions du règlement**. Par ailleurs, l'ordonnance par laquelle le projet de loi habilitera le gouvernement à améliorer la lisibilité du texte est la bienvenue, compte tenu de la complexité de la matière. Pour éviter toute forme d'insécurité juridique prolongée, la ratification de l'ordonnance doit intervenir au plus vite.

Néanmoins, ce projet de loi sur lequel votre rapporteure présente ses observations a le grand mérite de la cohérence et de l'intégration de nouveaux droits pour les citoyens européens dans le domaine numérique. Il pose les fondements d'une réflexion éthique qui doit nourrir notre travail de législateur pour aborder les bouleversements sociétaux provoqués par l'apport des nouvelles technologies.

I. LE RGPD (RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES) S'INSCRIT DANS LA CONSTRUCTION DU PARADIGME EUROPÉEN DE PROTECTION DES LIBERTÉS FONDAMENTALES DANS LE DOMAINE NUMÉRIQUE

A. LA MODERNISATION DU CADRE JURIDIQUE APPLICABLE À LA PROTECTION DES DONNÉES PERSONNELLES

1. Une adaptation aux nouvelles technologies…

Le cadre juridique européen applicable à la protection des données personnelles s'est d'abord appuyé sur une directive, définissant les grands principes qui s'appliquent encore aujourd'hui (1). En reprenant une formulation proche de celle de l'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, selon lequel « l'informatique doit être au service de chaque citoyen », la directive affirmait dans son deuxième considérant que « les systèmes de traitement de données sont au service de l'homme ; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus ».

L'évolution rapide des technologies de la communication et de l'information a toutefois rendu obsolète relativement rapidement un certain nombre de dispositions issues de la directive et transposées en droit français - avec quelques années de retard – par la loi de 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (2). En particulier, l'émergence du web 2.0 avec la collecte massive de données, leur transfert de plus en plus rapide et inévitable entre les différentes entreprises, par l'usage du *cloud computing*, ont nécessité de repenser les modalités de protection des droits fondamentaux des citoyens tout au long de la vie de la donnée en mettant en place des règles juridiques robustes face à l'évolution rapide et constante des technologies de la donnée et du web.

Il convenait par ailleurs, en respectant ainsi l'objectif établi dès la directive de 1995, d'unifier les normes au niveau européen pour assurer une protection aussi harmonisée que possible des droits des citoyens tout en facilitant

---

(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

(2) 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.

autant que possible la stabilité économique et la lisibilité des entrepreneurs [(1)]. L'objectif de protection maximale de la vie privée a été étendu aux contenus échangés par le biais des communications électroniques en 2002, complétant ainsi les garanties quant à l'exercice des droits fondamentaux dans le domaine digital [(2)].

Le texte du règlement général de protection des données (RGPD) [(3)] a fait l'objet d'une première communication de la Commission en 2010 [(4)], initiant alors un long parcours de négociations.

La capacité de l'Union à légiférer en matière de protection des données personnelles tient avant tout à l'intégration de ce principe à l'article 8 de la Charte des Droits Fondamentaux, au même titre que la protection de la vie privée [(5)]. La reprise à l'article 16 du TFUE [(6)] (Traité sur le fonctionnement de l'Union européenne) des règles de protection des données personnelles découle directement de la force juridique conférée à la Charte des Droits Fondamentaux par le Traité de Lisbonne, et notamment de son article 8.

2. …dans le contexte du marché unique du numérique

Les ambitions de Jean-Claude Juncker dans le domaine numérique, traduites dans la lettre de mission adressée au Commissaire en charge, se sont déployées dans la stratégie pour un marché unique du numérique [(7)]. Cette dernière s'est appuyée sur trois piliers :

---

(1) Considérant 3 de la directive 95/46/CE : considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés

(2) Directive 2002/58/CE du 12 juillet 2002 « vie privée et communications électroniques ».

(3) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

(4) Communication de la Commission européenne « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM (2010) 609 final du 4 novembre 2010.

(5) 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

(6) 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

(7) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, «Stratégie pour un marché unique numérique en Europe » COM(2015) 192 final.

- améliorer l'accès en ligne pour les consommateurs et les entreprises dans toute l'Europe ;

- créer un environnement propice et des conditions de concurrence équitables pour des services innovants et des réseaux numériques avancés ;

- maximiser le potentiel de croissance de l'économie numérique.

Ces trois domaines visaient avant tout à lever toute barrière nationale jugée inutilement restrictive, voire discriminatoire, dans la plupart des secteurs touchés par la digitalisation. Or, la Commission est partie du constat suivant : « *les technologies de l'information et des communications (TIC) ne sont plus un secteur économique parmi d'autres, mais elles constituent désormais la base sur laquelle reposent tous les systèmes économiques novateurs modernes. Au quotidien, au travail et dans notre vie sociale, l'internet et les technologies numériques transforment notre manière de vivre et de travailler en pénétrant tous les secteurs de l'économie et de la société. »*

La croissance des activités numériques en Europe est désormais indissociable d'actions de régulation, dans des domaines aussi variés que la protection des contenus culturels en ligne, la lutte contre les contenus haineux ainsi que les fausses informations ou encore une fiscalité adéquate et juste pour les entreprises numériques. Mais cet effort de régulation a sans doute été le plus important dans le domaine de la protection des données personnelles, ce dernier ayant été à juste titre considéré comme prioritaire pour assurer la sécurité et la confiance des citoyens dans l'économie numérique.

3. La difficulté des négociations, qui tient notamment à l'ampleur des enjeux, a abouti à un texte hybride

Il a fallu près de quatre ans pour aboutir au règlement dont le projet de loi relatif aux données personnelles s'assure de la bonne application dans la législation française. Les négociations qui furent occasionnées par ce texte tiennent tant à l'ampleur du secteur concerné, au caractère sensible des données personnelles, lorsqu'elles touchent à la santé ou à la défense nationale, qu'à l'intense activité de nombreux groupes d'intérêt représentant les acteurs du numérique [(1)]. Ce n'est en effet qu'après de nombreuses réunions sectorielles que le Conseil Justice et Affaires Intérieures (JAI) a validé l'ensemble du règlement. Les trilogues qui s'en sont suivis ont abouti le 4 mai 2016. Le règlement, publié le 21 mai 2016, doit entrer en vigueur deux ans après, afin de laisser aux entreprises et aux administrations concernées le temps de s'adapter.

(1) Barreau, Catherine. « Le marché unique numérique et la régulation des données personnelles », Annales des Mines - Réalités industrielles*, vol. août 2016, n° 3, 2016, pp. 37-41.*

a. La souveraineté numérique : l'application extraterritoriale du règlement

La mise en place du RGPD se justifie par le contexte dans lequel l'économie numérique mondiale se développe désormais. La dimension européenne relève de l'évidence pour quiconque compare le tissu économique continental aux acteurs dominants américains et chinois. Les GAFAM (1) et les BATX (2), en miroir, définissent par leurs activités et leurs parts de marché des standards qui ont un impact direct sur les régulateurs nationaux. En l'absence d'acteurs économiques comparables, l'Union européenne a fait le choix de définir des standards continentaux destinés à s'appliquer à tous les acteurs numériques qui exercent leur activité en Europe ou visent des clients européens.

Or la maîtrise de leurs données par les citoyens européens est un enjeu de souveraineté nationale et désormais européenne. C'est cette logique de protection maximale des droits fondamentaux des citoyens en ligne qui a motivé également la dimension extraterritoriale du règlement, dans la mesure où il « s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union », mais aussi « au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

b) 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 (3). »

Il demeure cependant que cette application extraterritoriale est soumise à un certain flou qui pourrait en atténuer la portée. En effet, outre le fait que la vérification de son application dans les pays tiers demande une forte collaboration entre les autorités nationales de protection des données personnelles, la désignation d'un correspondant au sein des responsables de traitement des pays tiers ne s'appliquerait pas en cas de traitement occasionnel des données, laissant à ces entreprises la libre appréciation de ce qu'est un traitement occasionnel.

Toutefois, la définition à l'échelle continentale de standards communs ne peut que renforcer le rôle moteur de l'Union européenne dans la mise en place d'un cadre réglementaire mondial. Le RGPD a été adopté alors que le Conseil de l'Europe révisait la Convention n° 108 sur la protection des données, que l'OCDE adaptait ses lignes directrices relatives aux données personnelles et que l'APEC,

(1) Google, Amazon, Facebook, Apple, Microsoft.

(2) Baidu, Alibaba, Tencent, Xiaomi.

(3) Article 3 du RGPD.

organisation de coopération dans la région de l'Asie-Pacifique, développait son propre cadre juridique en la matière. L'Union européenne a eu ici l'occasion de développer un système sans précédent, fondé sur un ensemble de principes dont l'application est assurée de manière coordonnée et décentralisée par les autorités de régulation nationale, de manière à respecter la subsidiarité et à mettre en valeur l'expertise de ces agences.

b. Un règlement autorisant des marges de manœuvre nationales

Toutefois, c'est en vertu de ces longues négociations que le texte final est une innovation en lui-même, un véhicule hybride entre règlement et directive. La volonté de la Commission européenne pour aboutir à une harmonisation aussi large que possible explique le maintien de la forme d'un règlement, pour définir un standard européen cohérent. La Commission a en effet fait le constat selon lequel la première directive de 1995 relative à la protection des données personnelles a entraîné une trop grande dispersion normative entre les États membres, aboutissant à fausser la concurrence et à empêcher les autorités de régulation à exercer leur activité de manière efficace. Le niveau de protection des droits et libertés des personnes physiques à l'égard du traitement de leurs données devant être équivalent dans tous les États membres, **votre rapporteure se félicite de ce que la forme du règlement ait été préservée**. Elle prend également acte de ce que certains points d'achoppement ne pouvaient faire l'objet d'un accord au Conseil.

C'est donc une méthode innovante qui a été inscrite dans le texte final. Ainsi que le développe le dixième considérant, « *en ce qui concerne le traitement des données à caractère personnel nécessaire au respect d'une obligation légale à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. »* Les marges de manœuvre nationales s'appliquent également à des déclinaisons sectorielles, telles que les données sensibles.

c. Un travail suivi pour assurer la plus grande harmonisation possible

Ces marges de manœuvre sont encadrées par un organe, le **G29**. Ce groupe de travail, institué par les articles 29 et 30 de la directive 95/46/CE, regroupe l'ensemble des autorités nationales de régulation et est actuellement présidé par la présidente de la CNIL, Isabelle Falque-Pierrotin. Le but de cette organisation est plus globalement de contribuer à l'élaboration des normes européennes en matière de protection des données, par des instruments de droit souple tels que des recommandations. Dans le cadre du RGPD, les recommandations portent sur les marges de manœuvre nationales et permettent d'indiquer à la fois les bonnes pratiques ainsi que de favoriser une harmonisation aussi grande que possible. C'est ainsi que le RGPD aboutit à la formalisation de ce groupe dans un **Comité européen de protection des données**, dont la

composition et les missions sont définies à l'article 68. Il a vocation à se substituer à l'organe actuel, en tant qu'organe indépendant de l'Union, doté de la personnalité juridique et composé du chef de chaque autorité de contrôle nationale ainsi que du Contrôleur européen de la protection des données [(1)].

Ce comité aura notamment pour missions de surveiller et garantir la bonne application du règlement, en bonne intelligence avec les autorités nationales, et sans préjudice de leurs propres capacités, de conseiller la Commission européenne dans le domaine de la protection des données personnelles, mais aussi de publier lui-même des instruments de « droit souple », tels que des lignes directrices ou des recommandations dans différents secteurs limitativement définis, afin de faciliter dans l'ensemble une mise en œuvre souple des dispositions du règlement.

Votre rapporteure y voit un outil supplémentaire de protection contre les divergences des législations nationales, mais rappelle que, compte tenu des nombreuses zones qu'il reste à préciser, les États membres et les autorités de contrôle national seront amenées à travailler en bonne intelligence pour définir un corpus jurisprudentiel issu de l'application pratique du règlement.

Outre la fondation de principes clairs et modernisés, le règlement innerve un certain nombre de champs cruciaux en matière de protection des données personnelles, tels que celui des données de santé et définit les meilleures méthodes pour s'assurer d'un degré élevé de protection des données des citoyens tout en limitant le fardeau économique que la nécessaire mise en conformité pourrait faire peser aux entreprises.

B. DE NOUVEAUX DROITS POUR UNE RESPONSABILITÉ ACCRUE DES RESPONSABLES DE TRAITEMENT

S'il est difficile de résumer en quelques traits un texte de près de cent articles, destinés à mettre en place un schéma juridique clair et solide pour la protection des données personnelles à l'échelle de l'Union, votre rapporteure souhaite rappeler les droits des personnes qui y sont rappelés ou consacrés, ainsi que l'inversion de la logique dans les dispositifs de contrôle.

1. Assurer le respect de la vie privée et la maîtrise des données

En premier lieu, le règlement consacre son troisième chapitre aux droits des personnes concernées par le traitement des données personnelles, soit toute personne physique identifiée ou identifiable par le biais de ce traitement. Sont ainsi renforcés des droits préexistants, tels que le droit à la transparence des informations et des communications relatives au traitement des données à caractère personnel, l'accès à ces mêmes données auprès du responsable de traitement, mais aussi le droit à la limitation du traitement en cas d'inexactitude des données ou de traitement illicite, entre autres.

(1) Article 68 du RGPD.

Toutefois, votre rapporteure souhaite souligner deux types de droit représentatifs de l'esprit dans lequel le RGPD a été négocié. Le premier, inscrit à l'article 17, relève du droit à l'effacement ou du « droit à l'oubli ». Ce droit se rattache à la protection classique de la vie privée, mais son intégration dans le RGPD est particulièrement poussée. Alors que le droit au déréférencement avait été introduit par la CJUE dans un arrêt notoire de 2014 [(1)], l'article 17 du règlement met en place une double obligation pour les responsables du traitement et les sous-traitants : il doit effacer, dans les meilleurs délais, les données à caractère personnel qu'un citoyen lui demande de supprimer [(2)] mais aussi, compte tenu de ses capacités techniques et du coût que cela peut représenter, prendre toute mesure raisonnable pour informer, lorsqu'il a rendu les données publiques, les autres responsables de traitement de la demande d'effacement.

Le droit à la portabilité des données, quant à lui, garantit aux personnes concernées la possibilité de recevoir des données à caractère personnelles les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine. Ces personnes ont le droit de transmettre ces données à un autre responsable du traitement sans que celui auquel les données à caractère personnel ont été communiquées y fasse obstacle, dès lors que ce traitement est automatisé et fondé sur le consentement, tel que défini par le RGPD [(3)].

Ces deux droits spécifiques au traitement automatisé des données en ligne assurent un meilleur contrôle aux citoyens de leurs données, de leur fourniture auprès d'un responsable de traitement, à leur suppression. Cela est d'autant plus vrai qu'ils ne font pas l'objet de marges de manœuvre nationales et tous les citoyens de l'Union en bénéficient de la même manière.

Ces nouveaux droits, fondamentaux pour la mise en pratique d'un cadre de vie privée mais aussi pour l'ouverture possible d'une concurrence entre les offres de services, ne pourront être mis efficacement en œuvre que si des techniques de traçabilité des données et des standards de formats de données voient rapidement le jour. Par ailleurs, ces droits connaissent des limitations. Il s'agit d'une part du droit à l'information, pour le « droit à l'oubli » et d'autre part du droit de la propriété intellectuelle pour la portabilité des données. À noter que dans sa mise en œuvre actuelle, le « droit à l'oubli » repose essentiellement sur l'interprétation qu'en font les plateformes elles-mêmes et qu'il serait souhaitable que les autorités de contrôle exercent davantage leur droit de régulation.

Le règlement instaure également une protection spécifique pour les enfants, déterminée à l'article 8 et examinée ci-après.

---

(1) CJUE, GC, 13 mai 2014, Google Spain SL et Google Inc.

(2) Un certain nombre de critères encadrent toutefois cette demande. Cela ne peut être le cas que lorsque les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ou que la personne concernée retire son consentement au traitement des données.

(3) Article 20 du RGPD.

2. Garantir techniquement un traitement adapté et proportionné des données

La meilleure protection possible de la vie privée en ligne est par ailleurs assurée techniquement par des dispositions telles que **la protection des données dès la conception** et la **protection des données par défaut**.

Le responsable de traitement, dans le premier cas, compte tenu d'un ensemble de critères tels que le coût de mise en œuvre ou la finalité du traitement, doit appliquer, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du règlement (1).

Dans le second cas, le responsable de traitement met en œuvre également des mesures techniques, pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (2).

Ces deux types de traitement pourraient être avantageusement signalés et contrôlés par un dispositif de certification, tels que le proposent le règlement et le projet de loi, dans son premier article.

3. Une inversion de la logique de contrôle et de responsabilité

Cet ensemble de principes est mis en œuvre par les responsables de traitement eux-mêmes, en premier lieu, selon une logique de confiance et de responsabilisation des acteurs privés par les autorités publiques. Les responsables de traitement doivent se conformer à une série de mesures de précaution, via la nomination de « délégués à la protection des données (3) », l'adoption de codes de conduite, le respect des mécanismes de certification et surtout la notification des failles de sécurité à l'autorité de contrôle ainsi qu'aux personnes concernées. Les régimes d'autorisation et les prohibitions absolues tombent donc pour la plupart d'entre elles, et le texte invite l'ensemble des acteurs à réfléchir selon une logique d'évaluation des risques et de responsabilité plutôt que d'autorisation et de surveillance.

Les autorités de contrôle, à l'instar de la CNIL (Commission Nationale de l'Informatique et des Libertés), doivent désormais accompagner les acteurs vers le

---

(1) Article 25 du RGPD.

(2) Ibid.

(3) Article 37 du RGPD, ce délégué doit être désigné en tout état de cause si le traitement est effectué par une autorité publique ou un organisme public, à l'exception des activités juridictionnelles, lorsque les activités du responsable privé du traitement ou de son sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique des personnes concernées, ou lorsque ces mêmes activités consistent à traiter des données relatives à des condamnations pénales ou susceptibles de révéler des caractéristiques ethniques, politiques, religieuses ou syndicales, voire génétiques, des personnes.

traitement le plus respectueux possible des données personnelles, par la diffusion de référentiels de bonnes pratiques et de conseils.

En échange de cette libération du régime d'autorisation préalable, les autorités nationales de régulation disposent de pouvoirs d'investigation et de sanctions renforcées. En fonction de la violation constatée, l'amende administrative peut s'élever jusqu'à vingt millions d'euros, ou de 2 % à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Cette inversion de paradigme s'appuie sur une logique fondée désormais sur la gestion du risque.

4. Une adaptation aux risques

La réduction des formalités préalables, propre au régime d'autorisation, au profit d'un système de contrôle *ex post* et des sanctions afférentes, ne fait pas l'économie d'une différentiation en fonction des risques traités.

L'évaluation des risques relève au premier chef de la CNIL, qui se voit confier des missions autres que celles qui étaient inscrites jusqu'alors dans la loi. En particulier, les instruments de droit souple introduits à l'article 1er du projet de loi, tels que les lignes directrices, référentiels et autres recommandations, à destination des responsables de traitement ou des sous-traitants, visent à homologuer des comportements en fonction du risque de brèche dans le traitement des données personnelles. De la même manière, les analyses d'impact, auxquelles seront tenus les responsables de traitement en fonction des activités exercées, pourront être complétées par une évaluation du risque résiduel après étude d'impact. L'accompagnement de la CNIL auprès des acteurs privés doit les aider à se situer sur une échelle de risques et donc de prendre les mesures appropriées.

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

C'est pourquoi le régime d'autorisation a été maintenu par le règlement pour certains cas précis, tels que la possibilité d'un risque élevé. Le règlement prévoit en particulier que l'analyse d'impact auquel doit se conformer, compte tenu des capacités technologiques dont il dispose, le responsable du traitement, se justifie en raison de la nature élevée du risque auquel s'expose ce dernier. Puis, selon l'article 36 du règlement, le responsable du traitement est tenu de consulter l'autorité de contrôle préalablement au traitement si l'analyse d'impact indique

que le traitement en question présente des risques élevés, sauf à mettre en œuvre des mesures destinées à l'atténuer. En réponse, l'autorité de contrôle fournit un avis sous un délai contraint de huit semaines, potentiellement prolongé de six semaines à raison de la complexité du traitement.

Le projet de loi reprend dans son ensemble les logiques de responsabilisation des acteurs du traitement des données personnelles, y compris les sous-traitants, et de gradation des procédures en fonction des risques encourus. Il vise également une harmonisation européenne appréciable ainsi que des exceptions justifiées dans leur ensemble.

Votre rapporteure regrette toutefois des imprécisions sur certains points et un texte souvent difficilement lisible, du fait notamment de la multiplicité des sources juridiques et de la volonté de conserver l'architecture de la loi de 1978. L'ensemble est nécessairement générateur de complexité, puisque les dispositions d'application directe du règlement n'apparaissent pas dans le corps du texte. Dès lors, votre rapporteure encourage le Gouvernement, en vertu de l'article 20 de l'actuel projet de loi, à user de l'habilitation pour, dans un délai de six mois, procéder à la réécriture de l'ensemble de la loi du 6 janvier 1978 afin notamment d'améliorer son intelligibilité, de mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel.

II. LE PROJET DE LOI RELATIF AUX DONNÉES PERSONNELLES : UNE MODERNISATION BIENVENUE DU CADRE JURIDIQUE NATIONAL

A. LE CHOIX COHÉRENT D'UNE HARMONISATION EUROPÉENNE MAXIMALE

1. Le RGPD contient de larges marges de manœuvre nationales

Pour des raisons expliquées plus haut, le règlement laisse quelque 56 marges de manœuvre aux États membres, dans les nombreux domaines où l'harmonisation complète se révélait impossible. Ces marges de manœuvre concernent ainsi le régime des sanctions pénales applicables en cas de violation des principes du règlement (considérant 149), les critères de déclenchement des sanctions administratives ainsi que leur dimension (considérant 150) ou encore les limitations au traitement des données génétiques, biométriques ou concernant la santé (article 9).

Toutefois, votre rapporteure se félicite de ce que le projet de loi ne fait qu'un usage parcimonieux de ces exceptions, ce qui permet de respecter la logique d'ensemble du texte européen et de viser une harmonisation aussi grande que possible avec nos partenaires.

2. Un choix légistique cohérent mais peu clair

Cet usage mesuré des exceptions inscrites dans le corps du règlement apparaît dans les choix légistiques. Ainsi, loin de recopier le règlement sur les nombreux aspects traités par ce dernier, le texte se contente d'éliminer les dispositions contraires. De même, la divergence que le Gouvernement choisit de mobiliser par rapport au texte européen permet de moderniser la lettre du texte. Ainsi, pour ce qui est des pouvoirs d'enquête et d'investigation dont la CNIL est désormais la détentrice, **l'article 4 supprime la notion floue de locaux à usage professionnel,** pour étendre le contrôle à tous les lieux et locaux qui ne sont pas affectés en tout ou partie au domicile privé, évitant ainsi des interprétations difficiles pour des espaces qui ne sont ni à usage professionnel, ni une partie d'un domicile privé.

Cependant, force est de constater que la conciliation entre le respect de l'architecture globale de la loi n° 78-17 et l'adaptation des dispositions du règlement entraîne une certaine confusion d'ensemble, mais aussi des risques juridiques. Les différences dans le champ d'application de certains articles, tels que l'article 10 du projet de loi sur lequel votre rapporteure revient ci-après, peuvent amoindrir la clarté et l'intelligibilité de l'ensemble du texte. Sa bonne compréhension par les acteurs de l'économie numérique est toutefois d'autant plus cruciale qu'il s'applique à tous les organismes extranationaux qui traitent de données de personnes résidant en France.

Votre rapporteure comprend, à la lecture de l'article 20 du projet de loi, que le Gouvernement entend améliorer l'intelligibilité de l'ensemble de la législation applicable aux données personnelles. Elle partage l'avis selon lequel la France n'a que trop tardé à mettre en place un véhicule législatif adéquat, alors que le délai de transposition de la directive (UE) 2016/680 du 27 avril 2016 court jusqu'au 6 mai 2018 et que le RGPD lui-même entre en vigueur au 25 mai 2018. Il n'en demeure pas moins que les inadéquations entre les dispositions conservées de l'ancien texte et celles qui sont directement issues de l'adaptation au règlement ou de la transposition de la directive sont dommageables et sources d'insécurité juridique.

3. La pertinence du règlement quant aux libertés fondamentales : l'exemple de l'accès des mineurs aux plateformes

En vertu d'un choix légistique d'économie, de nombreux aspects d'application directe du règlement n'apparaissent pas dans le projet de loi. Il en va ainsi de la protection des données à caractère personnel des mineurs. Les dispositions inscrites à l'article 8 du règlement relatif aux conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information sont certes d'application directe, mais les États membres étaient libres d'y déroger sur un point précis : la fixation de l'âge du consentement au traitement des données personnelles. Le règlement fixe à 16 ans l'âge en dessous duquel ce consentement doit être recueilli auprès des titulaires de la responsabilité parentale, mais prévoit que les États membres peuvent descendre jusqu'à l'âge de 13 ans. Si la France n'a pas fait un tel choix, l'Espagne ou la République tchèque ont choisi de faire usage de cette marge de manœuvre et de fixer l'âge de l'accès à certains services de l'information, tels que les plateformes digitales ou les réseaux sociaux, à 13 ans. Le G29 explicite et recommande la manière dont les responsables de traitement peuvent gérer les situations de divergence entre États membres sur l'âge de consentement, mais encourage les États membres à conserver une approche harmonisée en la matière [(1)].

Votre rapporteure souhaite apporter un certain nombre de précisions sur ce point. En premier lieu, du fait de la divergence des choix entre les différents États membres, les responsables de traitement et les sous-traitants devront en effet, pour cette matière comme pour d'autres, rester attentif aux différentes normes nationales et endurer le coût d'information engendré par cette situation. Par exemple, le projet de loi actuellement discuté en Estonie prévoit que l'âge du consentement soit porté à 14 ans, en vertu de l'article 33 du Code pénal estonien, selon lequel une personne peut être jugée légalement comptable de ses actes à partir de cet âge-là [(2)].

Il paraît d'autre part difficile de croire, malgré le recrutement de milliers de modérateurs sur des plateformes telles que *Facebook* pour « chasser » les

(1) Guidelines on Consent under Regulation 2016/679adopted on 28 November 2017. 17/EN WP259.

(2) Le texte en cours de discussion réformera l'actuelle Isikuandmete kaitse seadus.

comptes des enfants les plus jeunes, que la pratique numérique des mineurs de moins de seize ans, sera respectueuse de ces dispositions. Les autorités de contrôle, tout comme les prestataires techniques et les responsables de traitement, ne disposent pas de moyens, dans l'état actuel des avancées technologiques, pour vérifier que des mineurs de moins de seize ans n'usurpent pas le consentement au traitement de leurs données personnelles, auquel seules peuvent normalement consentir les personnes titulaires de l'autorité parentale, sauf à demander une photocopie de la carte d'identité ou de tout autre document susceptible de prouver l'âge de l'internaute, pratique impossible à mettre en œuvre.

En tout état de cause, votre rapporteure estime que la détermination adéquate de l'âge du consentement doit prendre en compte la réalité de la pratique des adolescents sur internet. Compte tenu des grandes difficultés techniques pour vérifier la réalité du recueillement du consentement auprès des autorités parentales et du nombre d'internautes potentiellement concerné [(1)], il conviendrait de mettre davantage l'accent sur l'éducation au numérique plutôt que sur une limitation difficilement applicable de la navigation des adolescents en ligne. Éviter la fragmentation doit être de surcroît un objectif prioritaire dans l'adaptation des lois nationales au règlement européen. C'est dans cet esprit que le pré-projet de loi suédois relatif à la protection des données s'appuie sur l'exemple du droit américain, l'avis du Contrôleur européen de la protection des données, les travaux de la Commission préalables aux trilogues, pour fixer l'âge du consentement à 13 ans.

Dès lors, votre rapporteure estime que, à l'instar du choix que semblent faire d'autres pays tels que la République tchèque ou l'Irlande, il conviendrait d'abaisser la limite d'âge relative au consentement à 13 ans, et appuyer cette position auprès des institutions européennes dans le cadre des échanges de bonne pratique actuellement mises en place par la Commission européenne.

Toutefois, en contrepartie de cet assouplissement, les modalités de contrôle des responsables de traitement doivent être d'autant plus renforcées et les informations à destination des utilisateurs finaux exposées clairement. Les adolescents doivent être en mesure de connaître les fins auxquelles leurs données personnelles sont traitées, ainsi que la manière dont elles le sont. À ce titre, ainsi qu'il est exposé ci-après, la mise en place d'actions de groupe en responsabilité ne peut que participer au renforcement des droits des citoyens, y compris mineurs, dans le domaine numérique.

(1) Selon une étude Ipsos du 29 avril 2015 sur les jeunes, Internet et les réseaux sociaux, les adolescents (13-19 ans) passaient en moyenne 13h30 par semaine sur Internet. À titre de comparaison, les enfants de 7 à 12 ans y passaient 5 h 30 en moyenne.

B. LA DÉFINITION D'UN ESPACE EUROPÉEN DE PROTECTION DES DONNÉES PERSONNELLES

La bonne application des droits de la personne, inscrits au chapitre III du règlement, dépend en grande partie de la bonne coopération des agences nationales en charge de la protection des données personnelles, qui disposent de l'expertise et des moyens pour ce faire.

1. La coopération entre les agences de protection des données personnelles

L'efficacité des actions de contrôle, d'instruction, d'enquête et de sanctions concernant le traitement transfrontalier des données personnelles, par un responsable de traitement établi ou non sur le territoire de l'Union européenne, est garantie d'abord par le principe de chef de filat. L'article 56 du règlement dispose ainsi que l'autorité de contrôle dont relève l'établissement principal ou unique du responsable du traitement, ou du sous-traitant, est compétente en premier chef pour effectuer le contrôle de l'usage des données. L'ensemble des agences concernées s'efforce d'échanger informations, bonnes pratiques et de prendre des décisions par voie de consensus. Pour ce faire, le règlement prévoit notamment que les agences ont un mois pour répondre à une demande d'information d'une autre autorité de contrôle.

Surtout, les autorités de contrôle peuvent mener des opérations conjointes, au sens de l'article 62 du règlement. Ces opérations, qui peuvent relever de l'enquête, de mesures répressives, peuvent inclure toutes les autorités des États membres dans lesquels le responsable du traitement ou le sous-traitant est établi, ainsi que ceux dans lesquels un nombre important de citoyens est susceptible d'être affecté par les opérations de traitement.

Concrètement, les modalités de coopération impliquent qu'une autorité de contrôle peut, avec l'autorisation de l'autorité de contrôle d'origine, conférer des pouvoirs d'enquête aux agents de l'autorité de contrôle d'origine participant aux opérations conjointes mais aussi accepter, pour autant que le droit de l'État membre « de destination » le permette, que les membres de l'autorité de contrôle d'origine exercent ces pouvoirs conformément au droit de l'État d'origine.

Le projet de loi prévoit en son article 5 l'adaptation du cadre national à ces nouvelles modalités de coopération continentale entre autorités nationales. En particulier, il prévoit que, lorsqu'une opération de contrôle conjointe se déroule sur le territoire français, des membres et agents des autres autorités de contrôle participant, le cas échéant, à l'opération peuvent être présents auprès des membres ou agents habilités de la Commission, agissant en tant qu'autorité de contrôle d'accueil. Suivant l'avis du Conseil d'État, le Gouvernement a inscrit dans le projet de loi la possibilité pour le président de la CNIL d'habiliter les agents issus des autorités de contrôle d'autres États membres pour exercer tout ou partie des pouvoirs d'enquête et d'instruction dont disposent les membres et agents de la

CNIL. Cette habilitation, par décision particulière, n'est ouverte qu'aux membres ou agents d'autorités de contrôle qui présentent des garanties comparables à celles dont disposent les membres ou agents de la CNIL dans l'exercice de leurs pouvoirs d'enquête ou d'instruction.

Une telle ouverture est en effet de nature à renforcer les possibilités concrètes de collaboration et à encourager les autorités de contrôle des autres États membres à confier aux membres et agents de la CNIL des pouvoirs similaires dans le cadre des enquêtes et instructions ayant lieu dans d'autres États membres. C'est le cas en Suède ou en Espagne, par exemple. Bien évidemment, en tout état de cause, le droit national trouve à s'appliquer pour ce qui est du contrôle des agents d'une autorité étrangère, comme par exemple l'interdiction de contrôler un domicile.

2. Le champ territorial d'application : une difficile coordination entre les États membres

Saisissant une marge de manœuvre ouverte par le RGPD, le Gouvernement a adapté le champ d'application territorial de la loi Informatique et libertés.

En vertu de l'article 3 du règlement, les dispositions qu'il contient s'appliquent :

- au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ;

- au même traitement de données relatives à des personnes concernées résidant sur le territoire de l'Union, par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, si les activités de traitement sont liées :

    - à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ;

    - 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.

- au même traitement lorsqu'il est effectué par un responsable de traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

Il s'agit d'une véritable innovation dans l'application d'un droit extraterritorial, étant entendu que la grande majorité des acteurs économiques responsables des traitements de donnée à caractère personnel sont établis en dehors du territoire de l'Union européenne.

Or, au titre de **l'article 5** de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les traitements de données à caractère personnel qui sont soumis à la loi sont définis de manière plus restrictive. Ils se distinguent entre deux catégories :

- les traitements dont le responsable est établi sur le territoire français ;

- les traitements dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne.

Le Gouvernement a fait le choix de fixer, à **l'article 8 du projet de loi**, un cadre territorial, non pas au champ d'application des dispositions du règlement, qui sont d'application directe dans tous les États membres, mais aux marges de manœuvre nationales, afin de pallier les difficultés relatives aux divergences entre législations nationales. Celles-ci ne peuvent en effet que découler de l'architecture actuelle du texte européen, malgré les lignes directrices du G29.

En l'absence de précision du règlement, alors que les marges de manœuvre concernent de nombreux aspects fixés par le texte, le projet de loi retient le lieu de résidence de la personne concernée pour l'ensemble des marges de manœuvre nationales, à l'exception des traitements mentionnés à l'article 85-2 du règlement.

Il s'agit ici de faire usage d'une marge de manœuvre décrite au considérant 153 du règlement, relative aux exceptions au nom des libertés d'expression et d'information, dont la liberté de la presse. Dans ce cadre, la logique est inversée et le droit applicable est alors celui de l'État membre dans lequel le responsable de traitement est établi.

Le choix global du Gouvernement est certes un choix cohérent, appliquant le principe du pays de résidence, qui sera le plus protecteur pour les droits fondamentaux des Français en ligne. C'est également le choix retenu par l'Allemagne, dans la section I (4) de sa propre loi sur les données personnelles, qui, si elle semble privilégier la notion d'établissement principal, étend le champ d'application des dispositions aux traitements privés si « le responsable de traitement ou le sous-traitant, bien que n'ayant pas d'établissement dans un État membre, relève du champ d'application du règlement. » L'article 4 du règlement intégrant la collecte dans les opérations de traitement, tout responsable établi dans un État membre de l'Union européenne qui collectera les données de citoyens allemands sera passible de la loi allemande de protection des données.

Votre rapporteure estime que cette précision permet une plus grande sécurité juridique, plutôt que de demeurer à droit constant, et garantit la bonne application de marges de manœuvre nationales aussi importantes que celles qui

s'appliquent aux données génétiques, biométriques ou encore aux régimes d'autorisation relatifs au répertoire national d'identification des personnes physiques (NIR) [(1)]. Elle est d'ailleurs essentielle en ce qui concerne le droit des enfants. Votre rapporteure soutient donc pleinement ce choix fort du Gouvernement.

Les États membres qui ont fait le choix d'appliquer leurs marges de manœuvre nationales au lieu d'établissement du responsable de traitement réfléchissent à la possibilité de mettre une règle de résidence au moins dans ce cas d'application.

Votre rapporteure considère toutefois que la rédaction proposée introduit une divergence dommageable au sein du champ d'application de l'article 5, dont la première partie, inchangée, ne s'applique qu'en fonction du lieu de résidence du responsable de traitement. Une telle divergence entre les dispositions de la loi issues des marges de manœuvre nationales et celles qui sont antérieures ne peut être que dommageable pour la bonne intelligibilité de l'ensemble. Il doit donc revenir à l'ordonnance habilitant le gouvernement de revoir l'ensemble du texte aux fins d'en assurer une meilleure intelligibilité et de faire en sorte que les acteurs économiques puissent connaître au mieux le champ d'application des marges de manœuvre nationales au moment du traitement des données. Cette question se pose avec d'autant plus d'acuité pour les traitements transfrontaliers. De plus, il conviendrait de faire en sorte que la protection des données ne s'applique pas uniquement en fonction de critères de résidence. Les personnes de passage de courte durée en France ou les travailleurs frontaliers, qui peuvent faire l'objet de nombreux traitements de données personnelles, ne seraient en effet pas concernés. Dès lors, la protection devrait s'étendre à toutes les personnes concernées se trouvant en France au moment du traitement de leurs données.

Elle souligne enfin les risques propres aux divergences entre les champs d'application nationaux. Il s'agira de trouver dans le cadre de la coopération entre les autorités de contrôle et les juridictions des modalités de conciliation entre les applications différenciées des marges de manœuvre nationales.

3. L'extension du régime de responsabilité aux sous-traitants

Le règlement introduit une responsabilité conjointe entre le responsable de traitement et le sous-traitant. Cette nouvelle notion est l'une des dispositions qui permet au règlement de viser l'ensemble des acteurs de l'économie numérique. À l'heure du *cloud computing,* la plupart des entreprises externalisent tout ou partie de leurs données. Les données personnelles ne seront donc bien protégées que si toute la chaîne de sous-traitance est responsabilisée.

La responsabilité qui incombe aux sous-traitants nécessite que le responsable du traitement soit, par défaut, sûr du sous-traitant avec lequel il traite,

(1) Article 9 du projet de loi.

et en particulier, qu'il présente les « garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement [(1)] ». Les relations sont régies par un contrat qui doit notamment, selon le règlement, définir « l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, en tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée [(2)]. » Les modalités contractuelles, si elles peuvent s'appuyer sur des modèles-types de la Commission européenne ou des autorités de contrôle, demeurent relativement souples mais sont essentielles à la définition claire des partages de responsabilités et donc par conséquent aux risques financiers encourus par les parties en cas de sanction.

La formulation retenue dans le projet de loi vise à distinguer les obligations s'appliquant aux sous-traitants en vertu du RGPD de celles qui leur incombent à raison de la directive (UE) 2016/680, transposée à l'article 19 du projet de loi. Ainsi, selon son article 10, les sous-traitants exerçant des activités prévues dans le cadre de l'article 35 de la loi actuelle doivent respecter l'ensemble des dispositions les concernant contenues dans le chapitre IV du règlement.

Dès lors, les traitements qui ne relèvent ni du règlement, ni de la directive, dépendent toujours de l'article 38 de la loi n° 78-17. Votre rapporteure estime que, dans la mesure où l'ensemble des activités des sous-traitants, sauf les fichiers dits « de souveraineté », soit les traitements mis en œuvre par l'État au titre de ses prérogatives de puissance publique, est compris dans le champ d'application du RGPD, elle prend acte de cette répartition. **Le principe de coresponsabilité entre le responsable de traitement et le sous-traitant, applicable aux fichiers d'identité numérique, par exemple, constitue néanmoins l'un des progrès les plus importants institués par le règlement**, en ceci qu'il permet d'adapter le régime de responsabilité aux nombreux transferts et traitements que divers acteurs font subir aux mêmes données personnelles, y compris dans le cadre de l'action de l'État.

C. LES NOUVELLES MISSIONS ET ACTIONS DES AUTORITÉS DE CONTRÔLE NATIONALES

1. La certification et les instruments de droit souple

Loin d'être uniquement des autorités titulaires de pouvoirs d'enquête et de sanctions, les autorités nationales en charge du respect et de la protection des données personnelles sont incitées par le règlement à accompagner les acteurs

(1) Ces garanties peuvent avantageusement prendre la forme de certifications.

(2) Considérant 81.

privés et à mener des actions de prévention. Cette dernière passe avant tout par des instruments dits de « droit souple », même si la violation des dispositions du règlement entraîne des sanctions, définies dans le projet de loi selon un nouveau référentiel. L'article 1er du projet de loi reprend un instrument crucial de l'arsenal dont pourra disposer la CNIL pour garantir en amont la conformité du traitement des données avec les dispositions du RGPD, à savoir la certification. Le règlement, s'il n'impose pas de telle mesure, encourage les États membres à adopter des systèmes de certification cohérents (1). Ces certificats doivent permettre de démontrer que les responsables de traitement et les sous-traitants respectent les droits et libertés des personnes concernées. Cette certification, d'une durée maximale de trois ans, ne vaut toutefois pas rescrit, puisqu'elle « ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant quant au respect » du RGPD (2).

À ce titre, l'article 1er du projet de loi confie à la CNIL la capacité d'agréer des personnes, des produits, des systèmes ou des procédures, afin d'en démontrer la conformité avec les dispositions du règlement, mais aussi des organismes certificateurs, sur la base de l'accréditation délivrée par le Comité français d'accréditation (COFRAC).

La CNIL pouvait déjà certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne (3), mais le projet de loi étend ses capacités de certification tout en les insérant dans un ensemble gradué d'instruments à la normativité faible (règlements types, prescription de mesures techniques et organisationnelles supplémentaires…).

Votre rapporteure salue la diversification des outils de la CNIL, et ce d'autant plus qu'il est admis que le droit souple est adapté aux évolutions technologiques actuelles, ainsi que le Conseil d'État l'affirme dans son étude annuelle de 2013 (4). Elle regrette toutefois deux aspects que délaisse l'article 1er dans son état actuel de rédaction.

En premier lieu, l'articulation des mécanismes de certification avec d'autres formes de droit souple déjà présents dans la loi relative à l'informatique, aux fichiers et aux libertés, n'est pas évidente. En particulier, la CNIL « délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de

(1) Article 42 du RGPD.

(2) Article 42 (4) du RGPD.

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

*(4) « La vie des entreprises accueille et utilise aussi le droit souple. Celui-ci y est souvent privilégié, pour des motifs à la fois économiques, juridiques et idéologiques, sans que ce terme ne revête de connotation péjorative : **le standard**, c'est-à-dire une référence commune dont on peut s'écarter en cas de besoin, apparaît préférable à la règle générale et contraignante. »*

l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label [1]. » Votre rapporteure estime qu'il existe ici une marge de progrès, et qu'en particulier l'intégration des modalités de labellisation dans le cadre de la certification permettrait de faire émerger un label unique, facilement reconnaissable et dont les entreprises qui en bénéficient peuvent immédiatement se prévaloir auprès de leurs clients comme de leurs fournisseurs.

Ensuite, votre rapporteure remarque la prégnance du fait national dans ce premier article. Si cela est moins gênant en matière de règlements types et, plus largement, de conseils aux entreprises, qui n'entraînent pas nécessairement de conflit de normes avec les autres autorités de contrôle, il n'en va pas de même en matière de certification. Au moment où, en matière de cybersécurité [2], émerge un système de certification européen fondé sur des standards communs, il est regrettable qu'un dispositif comparable et harmonisé ne soit pas proposé en matière de protection des données personnelles et de conformité au RGPD.

D'autre part, comme les représentants du CIGREF [3] l'ont expliqué à votre rapporteure, la CNIL pourrait avantageusement se renforcer avec une équipe de médiation du droit des données. En effet, les méthodes de médiation font leur preuve dans d'autres cadres pour régler les litiges entre entreprises et permettent d'éviter un trop grand contentieux. Ce type de techniques va s'avérer nécessaire pour régler des litiges tant entre responsables de traitement et sous-traitants qu'entre personnes concernées et plateformes, dans des cas tels que les demandes de mise en œuvre du « droit à l'oubli ». Votre rapporteure propose donc d'ajouter cette possibilité aux nouvelles missions de la CNIL.

2. Le traitement des données de l'État : une exception dommageable

Conformément à la logique de responsabilisation des responsables de traitement et des sous-traitants, le règlement prévoit que, « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes

---

(1) Article 11, alinéa 3c) de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) - COM(2017) 477 final : Article 43 : « Un système européen de certification de cybersécurité atteste que les produits et services TIC qui ont été certifiés conformément à ce système satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces produits, processus, services et systèmes. »

(3) Le CIGREF est une association loi 1901, créée en 1970, qui regroupe près de 145 grandes entreprises et organismes français dans tous les secteurs d'activité.

physiques [(1)] », ils mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Ces mesures techniques peuvent être de l'ordre de la pseudonymisation ou de l'anonymisation et le chiffrement des données à caractère personnel, ainsi que les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Pour assurer cette sécurité du traitement, le projet de loi prévoit, en son article 1er, la capacité de la CNIL à mettre en place des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données de santé. Elle peut ainsi « prescrire des mesures techniques et organisationnelles supplémentaires pour le traitement des données biométriques, génétiques et de santé » et « des garanties complémentaires en matière de traitement de données d'infraction ».

Votre rapporteure estime nécessaire que la CNIL puisse en effet disposer d'instruments plus contraignants que les seules recommandations en vue d'assurer la sécurité de traitement des données à caractère personnel. Elle comprend également l'exception faite pour « les traitements mis en œuvre par l'État, agissant dans l'exercice de ses prérogatives de puissance publique. » Il demeure que l'État, dans le champ de toutes ses autres actions, doit demeurer sous le contrôle de la CNIL. Votre rapporteure salue à ce titre le II de l'article 9 du projet de loi, qui maintient et ajoute un régime spécifique d'autorisation (décret en Conseil d'État pris après avis motivé et publié de la CNIL) pour certains traitements de l'État, à savoir les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. Cette disposition introduit une forme de complémentarité avec l'exonération précédente.

3. Le contrôle en ligne : une collaboration qui reste à construire

En complément des actions d'enquête et de contrôle sur pièce et sur place, tels que définis à l'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la CNIL procède également à des contrôles en ligne, tels que définis à l'article 44 de la même loi. Cette procédure, dont dispose la CNIL a été introduite par la loi n° 2014-344 du 17 mars 2014 relative à la consommation, en son article 105. Les agents de la commission peuvent ainsi procéder à toute constatation utile et « notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations. »

---

(1) Article 32 du RGPD.

Ce contrôle, qui doit être décidé par la Présidente de la CNIL via un ordre de mission, aboutit à un procès-verbal factuel décrivant la méthodologie employée ainsi qu'un procès-verbal de constatations en ligne, envoyé au responsable de traitement, avec ses annexes. À la suite d'un tel contrôle, la CNIL peut, le cas échéant, poursuivre les investigations via les instruments classiques que sont les contrôles sur pièce, sur place ou les auditions.

Ces contrôles en ligne portent avant tout sur la pertinence des données collectées [(1)], la bonne mention des informations à destination du public [(2)] ou encore la sécurité des données collectées et traitées [(3)]. En particulier, les contrôles visent à vérifier la conformité des sites internet à la recommandation adoptée par la CNIL en 2013 [(4)], concernant des critères tels que le nombre et la nature des *cookies* déposés sur le poste de l'internaute, les modalités d'information à destination du public en matière de *cookies* ou encore les modalités de recueil du consentement de l'internaute.

Cette question acquiert une actualité particulière au moment où le texte européen relatif à la protection de la vie privée dans les réseaux de communication est en cours de négociations [(5)]. Ce dernier, dont la date de publication semble devoir être repoussée au-delà de la date initialement prévue – soit la même date que la date d'application du RGPD, le 25 mai 2018 – doit notamment mettre en œuvre les dispositions propres au recueillement du consentement de l'internaute, tel que défini à l'article 7 du RGPD.

Votre rapporteure s'interroge sur les modalités de coopération des autorités de contrôle nationale quant à ce contrôle en ligne. **À ce titre, le projet de loi pourrait utilement prévoir les conséquences d'un contrôle en ligne sur des données recueillies de manière transfrontalière**.

4. Le référentiel de sanctions

Afin d'améliorer la visibilité des entreprises sur les modalités de sanction que pouvaient mettre en œuvre les autorités nationales et d'augmenter le montant potentiel desdites sanctions, le règlement met en place un référentiel, en son article 83, définissant le régime des amendes administratives.

La nouveauté tient d'abord à la mise en place de sanctions équivalentes dans tous les États membres, pour éviter tout « *forum shopping* » réglementaire. Le montant maximal de ces sanctions ainsi que les critères de fixation des

---

(1) Article 6 de la loi n° 78-17 du 6 janvier 1978.

(2) Article 32 de la loi précitée.

(3) Article 34 de la loi précitée.

(4) Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.

(5) Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») – COM (2017) 10.

amendes sont définis dans le règlement, charge ensuite aux autorités de contrôle nationales de les appliquer de manière proportionnée, en prenant en compte la nature de la violation des dispositions du règlement, le degré de responsabilité de l'organisme fautif ou encore le danger pour le respect des libertés fondamentales des personnes concernées.

L'autre aspect crucial, selon votre rapporteure, du règlement, dans ses dispositions d'application directe, tient à l'augmentation significative du montant maximal des amendes administratives. Celles-ci peuvent ainsi s'élever à 20 millions d'euros ou 4 % du chiffre d'affaires annuel de l'exercice mondial total de l'exercice précédent, en cas de violation :

- des principes de base du traitement, tels que le principe du consentement ;

- des droits et libertés de personnes concernées définis de l'article 12 à l'article 22 du règlement ;

- de transfert illicite de données à caractère personnel vers le destinataire situé dans un pays tiers ou vers une organisation internationale ;

- des obligations découlant du chapitre IX relatif à des situations particulières de traitement, impliquant la liberté d'expression et d'information ou l'accès du public aux documents officiels ;

- du non-respect d'injonctions ou de limitations du flux des données ordonnées par une autorité nationale de contrôle.

Votre rapporteure estime qu'il s'agit là d'un renforcement cohérent des modalités de sanction, corollaire nécessaire au nouveau régime applicable aux responsables de traitement et aux sous-traitants. Elle souhaite toutefois attirer l'attention des autorités de contrôle sur les traitements spécifiques mis en œuvre par les entreprises innovantes et les *start-up*. S'il n'est pas souhaitable de modifier le projet de loi dans le sens d'un allégement normatif pour ces entreprises sur le modèle des « bacs à sable » réglementaires [(1)], dès lors que le règlement ne prévoit pas ce type de marge de manœuvre nationale, la CNIL devrait continuer à procéder tel qu'elle le fait actuellement. Le dialogue en amont avec les porteurs de projet est en effet crucial pour améliorer les analyses d'impact fournies par les responsables de traitement et les aider à prendre en compte les risques inhérents à ce traitement. Ce type de démarche proactive dépend toutefois nécessairement des moyens mis à la disposition du régulateur. Votre rapporteure rappelle ainsi que la *Datainspektionen*, l'autorité de régulation suédoise, a reçu un budget d'environ 150 000 euros pour aider les entreprises à mettre en œuvre les dispositions du RGPD.

(1) Ce type de dispositif a été mis en place par l'ARCEP, dans le cadre de l'article L.40-1 du code des communications électroniques et des postes permet aux start-up qui le souhaitent, et plus largement à toute entreprise s'apprêtant à tester de nouveaux services, de bénéficier d'un allègement des obligations notamment liées aux attributions de fréquences et de ressources en numérotation.

5. Les limites du contrôle : l'opposabilité du secret professionnel

La possibilité d'opposer le secret professionnel aux contrôles des agents de la CNIL était déjà prévue dans la loi n° 78-17, en son article 21. Or, il s'agit de l'une des marges de manœuvre nationales laissées par le règlement, en son article 90 (1). Celle-ci permet de maintenir en l'état la plupart des dispositions déjà présentes dans la loi, à l'instar de l'Allemagne qui, dans sa loi, n'a pas fait usage de cette marge de manœuvre pour changer les modalités de protection du secret professionnel.

Le projet de loi permet toutefois une clarification de l'opposabilité des secrets au contrôle de la CNIL, étant donné que l'article 44 de la loi actuelle, selon lequel « 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 », pourrait laisser penser qu'il s'agit de la seule protection possible d'un secret face aux contrôles de la CNIL.

Votre rapporteure salue cet effort de clarification, qui distingue désormais l'opposabilité de trois types de secret :

- le secret médical, dans certaines situations strictement définies [(1)] ;

- le secret professionnel applicable aux relations entre un avocat et son client ;

- le secret des sources des traitements journalistiques.

Toutefois il est nécessaire de vérifier que les marges de manœuvre nationales d'application du secret professionnel ne freinent pas les possibilités de contrôle des autorités nationales en créant des distorsions entre États membres. En effet, même si la plupart d'entre eux restent au stade de la réflexion sur leurs projets de lois, la loi roumaine ne prévoit aucune restriction à l'accès aux locaux ou aux informations et le secret professionnel ne peut être opposé aux agents en charge d'inspections. À l'inverse, la loi belge est beaucoup plus protectrice [(2)].

---

(1) Pour ce qui est du secret médical attaché aux traitements nécessaires aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé, il ne sera plus exigé que ce soit seul un médecin qui puisse requérir la communication des données mais que cette communication ne peut être faite que sous l'autorité et en présence de ce dernier.

(2) « Une profession soumise au secret professionnel et pour qui il existe des règles légales particulières, l'inspecteur général et les inspecteurs ne peuvent accéder, sans la présence d'un représentant de l'ordre professionnel, à leurs locaux que moyennant un accord écrit de la personne contrôlée ou bien moyennant l'accord du juge d'instruction. Il s'agit de conditions cumulatives (telles que chez les médecins, avocats ou journalistes). »

D. UNE PROTECTION DES CITOYENS À CONSOLIDER

1. La limitation des droits dans le domaine numérique

L'économie générale du RGPD, ainsi que les lois portant adaptation de la législation nationale au nouveau régime européen de protection des données, visent la protection la plus grande possible des droits, anciens et nouveaux (droit à l'oubli et droit à la portabilité des données), consacrés dans le domaine numérique.

Il demeure toutefois que, pour des considérations d'ordre public, ces droits souffrent de limitations, justifiées, selon le règlement, si elles ne s'appliquent que 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* [(1)]. »

Cet ensemble de critères permettant de limiter l'exercice de droits aussi fondamentaux que le droit à l'information ou le droit d'accès aux données se traduit à l'article 23 du règlement. Ainsi, le droit de l'État membre auquel sont soumis responsables de traitement et sous-traitants peut limiter les droits et libertés inscrits au chapitre III du même règlement, sous la condition expresse de respecter des critères formels et des dispositions garantissant le bon exercice des libertés publiques dans le domaine numérique [(2)].

---

(1) Considérant 73 du RGPD.

(2) Les mesures doivent intégrer des dispositions spécifiques relatives notamment :

- *aux finalités du traitement ou des catégories de traitement ;*
- *aux catégories de données à caractère personnel ;*
- *à l'étendue des limitations introduites ;*
- *aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;*
- *à la détermination du responsable du traitement ou des catégories de responsables du traitement ;*
- *aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;*
- *aux risques pour les droits et libertés des personnes concernées ;*
- *au droit des personnes concernées d'être informées de la limitation, à moins que cela ne risque de nuire à la finalité de la limitation.*

La loi n° 78-17 prévoit elle-même un certain nombre de limitations à l'exercice de ces droits, comme en matière d'accès aux données, auquel le responsable de traitement peut légalement s'opposer si les demandes sont manifestement abusives, eu égard notamment à leur caractère répétitif ou systématique [(1)]. Le droit d'accès n'est pas garanti non plus lorsque les données à caractère personnel sont conservées sous une forme telle qu'aucune violation pouvant aboutir à une atteinte de la vie privée des personnes concernées n'est à craindre.

D'autres libertés peuvent évidemment aller à l'encontre de certains droits des personnes concernées. Ainsi, la liberté d'expression et d'information, des motifs d'intérêt public dans le domaine de la santé publique, des fins archivistiques dans l'intérêt public ou encore des fins scientifiques peuvent s'opposer à ce que soit mis en œuvre de manière absolue le droit à l'effacement ou à la rectification, tel qu'il peut découler de la jurisprudence de la CJUE ou du RGPD lui-même.

Le projet de loi s'appuie sur la grande marge de manœuvre qu'autorise l'article 23 du règlement pour introduire une dérogation supplémentaire à l'exercice des droits des personnes concernées. Il s'agit **de traiter des cas dans lesquels la communication d'une divulgation ou d'un accès non autorisé à des données est susceptible de présenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique, et lorsque sont en cause des traitements ou catégories de traitements nécessaires au respect d'une obligation légale ou à l'exercice d'une mission d'intérêt public.** Cette disposition s'inscrit dans le contexte actuel de menace terroriste et de détournement de données potentiellement cruciales. La divulgation de l'intérêt que présentent les données peut en effet attirer l'attention des organisations terroristes sur la valeur des données usurpées, le cas échéant.

D'autres États membres font usage des limitations prévues à l'article 23. Le texte estonien actuel prévoit ainsi que les pouvoirs publics peuvent traiter des données personnelles collectées initialement à d'autres fins, en vue d'établir l'existence d'une menace à l'ordre public, de contrer ladite menace ou encore pour assurer la bonne application des peines.

Votre rapporteure considère que la limite à l'exercice des droits des personnes contenue dans le projet de loi est appropriée, mais estime, globalement, qu'il convient de faire en sorte que les traitements mis en œuvre par l'État ne fassent pas l'objet d'un traitement préférentiel. À ce titre, elle estime que le Parlement devrait disposer d'un droit de regard accru sur le traitement des données à caractère personnel, avec l'assistance de la CNIL, à l'instar des débats qu'avait pu occasionner l'autorisation du fichier TES par le décret n° 2016-1460 du 28 octobre 2016.

---

(1) Article 39.

2. L'action de groupe : introduire des modalités de réparation

L'action de groupe constitue un recours très récent dans l'arsenal juridique national. Introduit dans un premier temps par la loi n° 2014-344 du 17 mars 2014 relative à la consommation, il était limité à la défense de groupes de consommateurs par une association de consommateurs agréée au niveau national. Applicable aux cas de vente de biens ou de fournitures de service, l'action de groupe devait être initiée par les consommateurs lésés, obtenant réparation par la suite en se signalant auprès de l'organisme condamné ou de l'association de consommateurs requérante.

Le champ d'application de l'action de groupe a été ouvert par la suite à d'autres domaines, tels que la santé [(1)], mais aussi à la lutte contre les discriminations, aux actions ayant une incidence sur l'environnement, et enfin, aux données personnelles [(2)]. Toutefois, dans ce dernier domaine, si l'action de groupe permet à « 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 », l'action ne peut viser exclusivement que la cessation du manquement. Il n'est donc pas possible d'introduire un recours en responsabilité à raison de la violation des données personnelles des utilisateurs d'un service de la société d'information [(3)].

Le RGPD prévoit plusieurs types de recours en cas de violation des dispositions relatives aux protections des données personnelles des utilisateurs ainsi que des nouveaux droits qu'il consacre. Inscrits dans le chapitre VIII, l'article 77 prévoit un droit d'introduire une réclamation auprès d'une autorité de contrôle, l'article 78 un droit à un recours juridictionnel effectif contre une autorité de contrôle et l'article 79 un droit à recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant, à chaque fois à raison d'une violation des droits inscrits dans le règlement.

Le projet de loi prend en compte, **dans son article 16**, les conséquences de l'ouverture de ces voies de recours en complétant la loi n° 78-17, qui prévoit déjà au 2 °c) de son article 11 la possibilité pour toute personne concernée de déposer une réclamation, une pétition ou une plainte auprès de la CNIL. Outre la possibilité introduite à l'article 1er du projet de loi, pour la CNIL, de présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application du règlement ainsi qu'à la loi n° 78-17 modernisée, le choix opéré par le Gouvernement a consisté à ouvrir l'action de groupe obligatoire, prévue à l'article 80.1 du règlement, aux associations qui étaient déjà mentionnées au IV de l'article 43 *ter* de la loi du 6 janvier 1978. C'est par ce biais que peuvent être exercés les droits susmentionnés inscrits aux articles 77, 78 et 79 du règlement.

---

(1) Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé et décret n°2016-1249 du 26 septembre 2016 relatif à l'action de groupe en matière de santé.

(2) Titre V de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.

(3) Article 43 ter *de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Le Gouvernement a renoncé par-là même à la possibilité d'introduire un recours en réparation pour compléter le dispositif prévu par la loi de modernisation de la justice au XXI^{e} siècle(1) .

La possibilité d'une action en réparation est pourtant ouverte dans plusieurs États membres. Ainsi, aux Pays-Bas, depuis 1993, les associations et les fondations peuvent engager une action en justice aux fins d'une réparation collective. Depuis 2005 et la promulgation de l'Acte des Actions Collectives, celles-ci peuvent de plus aboutir à une indemnisation commune. Ces actions de groupe, qui ne sont pas limitées à un domaine en particulier, doivent être issues d'un accord extrajudiciaire préalable entre les représentants des responsables du dommage et les représentants des victimes. Cet accord permet de fixer une indemnisation commune, avant son homologation par le juge. La jurisprudence des tribunaux néerlandais a fait évoluer le champ d'application de cette action de groupe, puisque des plaignants étrangers peuvent s'ajouter à une action, dès lors qu'un seul plaignant est domicilié aux Pays-Bas. D'autres types d'actions de groupe en responsabilité existent dans d'autres États membres, sous diverses modalités, comme en Italie ou au Royaume-Uni.

Les représentants de l'association UFC-Que Choisir ont expliqué à votre rapporteure le caractère crucial d'une telle action de groupe, et militent pour l'adjonction d'un préjudice moral en cas de violation de la protection des données personnelles. En effet, « *dès lors que les critères de mise en application de l'action de groupe sont définis de manière très stricte, une simple action de groupe en cessation, telle qu'elle est inscrite aujourd'hui dans la loi, ne sert à rien.* »

Cet ensemble laisse craindre à votre rapporteure une certaine inégalité dans les droits auxquels peuvent prétendre les citoyens européens au titre du RGPD. Elle regrette donc fortement le fait que le gouvernement n'ait pas profité de la révision de la loi n° 78-17 pour introduire une action de groupe en responsabilité, comme l'y autorise **l'article 80.1 du règlement.**

Votre rapporteure regrette également que le Gouvernement n'ait pas saisi l'opportunité offerte par l'article 80.1 du règlement pour adapter le droit existant. L'actuel article 43 *ter* de la loi n° 78-17 permet certes un droit de recours contre un responsable de traitement tel qu'il est inscrit à l'article 79 du règlement, mais sans mise en cause de la responsabilité, et n'introduit aucune possibilité de recours en responsabilité à l'égard de l'autorité publique de contrôle. De même, aucun organisme agréé ne peut introduire de réclamation au sens de l'article 77 du règlement.

En tout état de cause, votre rapporteure souhaite que la possibilité de mener des actions de groupe en réparation soit intégrée au projet de loi.

---

(1) Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle.

3. Les actions de médiation

L’esprit du règlement européen vise à accompagner les responsables de traitement et leurs sous-traitants dans leurs activités, de telle sorte que les droits des internautes soient garantis à tout moment. Cette responsabilisation doit être accompagnée, et notamment dans le cadre des litiges qui pourraient naître entre les responsables de traitement et les sous-traitants.

Les autorités de contrôle nationales sont encouragées à faire en sorte que le dialogue entre les professionnels permette d’éviter les contentieux de masse ou nés d’une mauvaise compréhension des dispositions du règlement.

Par ailleurs, la CNIL met déjà en place des actions proches de ce qui pourrait être qualifié de médiation. Ainsi, dans le cadre de l’instruction des plaintes reçues, les mesures d’avertissement, de mises en demeure, ainsi que la possibilité pour le responsable de traitement de présenter les modalités de traitement des données, dans le respect du contradictoire, réduisent grandement le nombre de sanctions. Celles-ci ne représentent qu’environ 2 % des affaires traitées, soit 15 à 20 par an.

Votre rapporteure estime toutefois qu’il y aurait intérêt à mettre en place des mesures de médiation, sur le modèle du Médiateur des entreprises, dans une phase précontentieuse entre professionnels. Ce médiateur pourrait être la CNIL ou un tiers, sans préjudice de la capacité de toute personne concernée ou acteur économique de saisir la CNIL directement, comme le prévoit l’article 77 du règlement.

TRAVAUX DE LA COMMISSION

La Commission s'est réunie le 18 janvier 2018, sous la présidence de Mme Sabine Thillaye, Présidente, pour examiner le présent rapport d'information.

Mme Christine Hennion, rapporteure. Le projet de loi sur lequel notre commission présente des observations adapte la législation nationale au Règlement Général de Protection des Données, ou RGPD, et transpose la directive 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 et de sanctions pénales.

Après 4 ans de négociation, le Règlement général de protection des données doit s'appliquer d'ici le 25 mai 2018 et représente un effort sans précédent, et sans doute jusque-là inégalé, de définir un standard commun en la matière. La capacité de l'Union à légiférer en matière de protection des données personnelles tient avant tout à l'intégration de ce principe à l'article 8 de la Charte des Droits Fondamentaux repris à l'article 16 du Traité sur le fonctionnement de l'Union européenne au titre de la vie privée.

Ce texte, de portée mondiale, puisqu'il devra être appliqué par tout organisme traitant les données personnelles des résidents européens, est fondateur pour la garantie des libertés dans le monde numérisé du XXI^{e} siècle. La restauration de la confiance des utilisateurs dans le domaine du numérique aura pour conséquence directe le développement des entreprises au sein du marché unique numérique. Les évolutions technologiques extrêmement rapides nécessitent une vigilance accrue du respect à la vie privée des personnes, de leurs libertés de citoyens et de notre souveraineté numérique. Ce règlement, et ses marges de manœuvre nationales introduisent un renversement de la logique de contrôle. Le texte nous fait passer d'un régime d'autorisation, pour un grand nombre de traitements de données, à un régime de responsabilisation des entreprises et administrations.

Les organismes devront évaluer les risques et les impacts sur la vie privée afin de prendre des mesures proportionnées qui pourront ensuite être contrôlées par les autorités nationales. En d'autres termes, nous passons d'un droit dur à un droit souple, à l'instar des législations anglo-saxonnes. Les CNIL européennes doivent désormais guider et accompagner les responsables de traitement. En complément de ces actions de prévention, les autorités de contrôle nationales auront désormais la possibilité d'infliger des sanctions, en fonction de la gravité de la violation et des risques pour la vie privée des personnes concernées, qui pourront aller jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires mondial consolidé de l'exercice précédent.

Ce Règlement part de la réalité du fonctionnement des marchés du numérique. Il corrige des failles de la précédente directive en renforçant les droits existants des citoyens et en en introduisant de nouveaux. C'est ainsi que les droits d'accès aux données et à l'information sont mieux garantis, la notion de consentement éclairé est très largement renforcée, tandis que le droit à l'effacement, ou « droit à l'oubli », et le droit à la portabilité des données sont mis en place.

Le RGPD est un texte hybride, qui laisse plus d'une cinquantaine de marges de manœuvre nationales. Le projet de loi met en application un certain nombre d'entre elles. Si la plupart sont justifiées, je demeure convaincue qu'il faut rechercher l'harmonisation la plus grande possible avec nos voisins européens. Il en va de l'efficacité du marché unique du numérique. Le règlement prévoit ainsi la collaboration des autorités nationales de contrôle pour s'assurer de l'application uniforme de ses dispositions à l'échelle du continent. Plutôt que de mettre en place une CNIL européenne, le choix a été fait d'un mécanisme de cohérence chapeauté par un Comité européen de protection des données, composé des présidents de chacune des autorités nationales. Les CNIL seront également amenées à conduire des enquêtes conjointes, dès lors que le responsable d'un traitement de données mis en cause exerce ses activités dans plusieurs États membres.

Plus largement, les divergences réglementaires entre les États membres ne doivent pas se faire au détriment des opérateurs économiques, et notamment des plus petits d'entre eux qui n'ont pas les capacités organisationnelles et juridiques pour s'adapter non seulement au RGPD mais encore à 27 choix différents effectués au titre des marges de manœuvre nationales. Les projets de loi français et allemands ont fait le choix d'appliquer les marges de manœuvre nationales aux personnes résidant dans leurs pays. Mais de nombreux autres États membres ont fait le choix inverse et appliquent leurs droits en fonction du lieu d'établissement des responsables de traitement ou des sous-traitants. Que se passera-t-il alors quand un responsable de traitement établi dans un tel État membre collectera et traitera des données personnelles d'un citoyen français ? Il faut réfléchir à un moyen d'articuler les normes nationales, pour éviter toute forme de carambolage contentieux, dans des matières aussi fondamentales que la protection de la vie privée.

Le gouvernement a fait le choix de se restreindre dans de nombreux domaines. J'estime toutefois qu'il aurait été pertinent de faire usage des marges de manœuvre à deux reprises, et ce d'autant plus qu'il est permis d'espérer une harmonisation européenne en la matière.

Le premier cas relève de l'âge du consentement au traitement des données personnelles. Les mineurs doivent être éduqués au numérique, être guidés dans leurs premiers pas, tant dans le cadre familial que dans le cadre scolaire. Compte tenu des pratiques actuelles des adolescents, la demande d'un consentement auprès des autorités parentales jusqu'à l'âge de 16 ans paraît difficilement contrôlable. Enfin, mes entretiens avec la Commission européenne m'ont laissé

comprendre qu'il y aurait une grande divergence entre les États membres quant à la fixation de l'âge minimal de consentement. Il me semblerait pertinent, dès lors, de descendre cet âge à 13 ans, de l'harmoniser à l'échelle de l'Union européenne, d'éduquer les adolescents sur les conséquences de leurs pratiques sur internet et d'obliger les sites à fournir une information claire, plutôt que de les en exclure en l'absence du consentement des parents.

Le second cas porte sur les actions de groupe. Cet instrument juridique, qui permet de lier de nombreuses plaintes individuelles, a été introduit en droit français par la loi sur la consommation de 2014, dite loi Hamon, puis étendue en 2016 par la loi relative à la justice au XXI^{e} siècle à divers domaines, dont les données personnelles. Cette dernière action de groupe se limite toutefois à la cessation du traitement, ce qui limite fortement son intérêt. Or, le règlement autorise les États membres à mettre en place des actions de groupe en réparation en cas de violation de ses dispositions, permettant ainsi une juste indemnisation des personnes concernées. Ce type d'action de groupe existe déjà dans un certain nombre d'États membres, tels que les Pays-Bas et peut être étendu à partir de là aux résidents des autres états membres. La prise en compte de la réparation serait d'autant plus indispensable que l'âge du consentement serait abaissé à 13 ans.

Afin de garantir en amont la conformité du traitement des données avec les dispositions du RGPD, le règlement encourage les États membres à adopter des systèmes de certification cohérents. Ces certificats doivent permettre de démontrer que les responsables de traitement et les sous-traitants respectent les droits et libertés des personnes concernées. Cette certification, d'une durée maximale de trois ans, « ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant quant au respect » du RGPD. J'encourage vivement la mise en place de ce système harmonisé au niveau européen, afin d'en augmenter l'impact et de diminuer les coûts pour les entreprises.

Je pense qu'il serait par ailleurs très utile de mettre en place des actions de médiation. Elles pourraient intervenir dans une phase précontentieuse et faire en sorte que les professionnels du secteur se parlent, dans l'esprit du règlement, ainsi qu'entre plateformes et particuliers. Ce dispositif pourrait revenir à la CNIL ou un organisme tiers, à condition toutefois que cette médiation soit facultative et que les moyens du régulateur soient adaptés à cette nouvelle fonction.

Enfin, je souhaiterais voir se mettre en place un système de « bac à sable » réglementaire. Ce système vise à alléger les contraintes pour favoriser l'innovation. Il permet d'expérimenter pendant un temps, puis de se soumettre à la législation en place une fois la phase d'expérimentation achevée. Ce bac à sable doit bien entendu être sécurisé.

Pour conclure mon propos, je souhaite souligner le rôle majeur de la CNIL dans l'application de ce règlement et, à ce titre, je souhaiterais que les moyens financiers et humains de cette autorité soient renforcés.

Telles sont les propositions que je porte sur ce projet de loi, dont je souhaite souligner encore la pertinence et qui permet à la France de participer au mieux à l'un des standards continentaux les plus avancés au monde en matière de protection des données personnelles. Je vous remercie.

L'exposé de la rapporteure a été suivi d'un débat.

Mme la présidente Sabine Thillaye. Merci beaucoup, chère collègue, pour ce rapport d'observations précis. Je reste quelque peu dubitative par rapport au choix de l'instrument juridique par l'Union européenne ; d'un côté, on a affaire à un règlement, de l'autre, pour l'espace de liberté, de sécurité et de justice, on a choisi la directive. Ce règlement donne une telle latitude aux États membres sur beaucoup de points très importants qu'il ressemble fort à une directive. Ce texte est par ailleurs à la croisée de deux objectifs contraires : la libre circulation des informations et une véritable protection des données personnelles.

Mme Marietta Karamanli. Madame la Présidente, je partage votre remarque sur ce point du choix du règlement par rapport à la directive.

Madame la rapporteure, je vous remercie des éléments que vous avez présentés. J'aurais souhaité faire quelques remarques. Tout d'abord, le projet est examiné en procédure accélérée, à l'instar de nombreux textes, et ce qui devrait être l'exception devient aujourd'hui la norme. Il est frustrant de travailler dans un calendrier si restreint, qui ne donne pas la possibilité de discuter en prenant le temps nécessaire. D'autre part, comme l'a noté le Conseil d'État, l'étude d'impact n'éclaire, en dépit de son volume, qu'assez peu les choix faits par le Gouvernement.

Je m'interroge sur le principe d'une autorisation préalable concernant les traitements automatisés, qui est remplacé par une auto-évaluation dont vous avez parlé dans votre rapport, avec les risques que cela induit de gérer des traitements de données avec un contrôle *a posteriori*. La CNIL voit son rôle évoluer, puisque le régime d'autorisation préalable n'est conservé que pour trois types de données : celles de la sécurité sociale, les données biométriques et génétiques, ainsi que les données de santé. Je souhaiterais savoir si vous avez pu avoir accès à des éléments de législation comparée au niveau européen sur ce sujet-là. Et plus précisément, quels sont les autres États européens qui passent ainsi d'un tel système d'autorisation préalable à celui d'une auto-évaluation ? Quels éléments ont été mis en évidence par les études d'impact menées dans les autres États membres ? Quels sont les bénéfices et les inconvénients de ce nouveau régime pour la protection des secteurs d'intérêt public sensibles ? Par ailleurs, le projet de loi ne traite pas de façon particulière des données en matière d'éducation et de scolarité. Je voulais avoir votre point de vue sur cette question.

Enfin, ce projet de loi fait l'impasse sur les travaux précédents menés par la commission des lois et par celle des affaires européennes, à savoir le droit à l'oubli et le droit à la portabilité des données qui devront être mis en œuvre par les responsables de traitement, conformément aux dispositions du règlement. Seul l'article 15 encadre la limitation des droits en posant comme condition que cette limitation respecte l'essence des libertés et des droits fondamentaux mais cette expression est particulièrement vague. Enfin, la manière, dont l'âge à partir duquel un mineur peut consentir à une offre directe de service sur les réseaux sociaux a été déterminée, n'est pas satisfaisante. L'âge fixé est 16 ans, mais pensez-vous que cette obligation sera respectée dans les faits ? Peut-être aurait-on pu suggérer dans le rapport de faire une distinction entre ce qui relève des activités ouvertes à des adultes et celles réservées à des jeunes, par exemple des jeux, ou des contenus culturels ? Je vous remercie en tous cas d'avoir travaillé sur ce sujet très complexe, mais qui touche, comme vous l'avez dit, Madame la Présidente, de plus en plus notre vie quotidienne. Il faut que nous restions très vigilants lors des discussions sur ce sujet au sein de l'hémicycle.

Mme Christine Hennion, rapporteure. Je vais d'abord aborder le point règlement *versus* directive. Effectivement, il aurait été possible de faire le choix d'une « directive », puisqu'il faut effectivement adapter la législation nationale pour chaque État membre. L'intention de départ était de recourir à un règlement pour avoir une harmonisation la plus large possible au niveau européen, d'en faire un standard et de tenir compte de la réalité du marché numérique. Cela rend difficile la compréhension du dispositif car, pour en saisir la portée, il faut avoir trois textes sous les yeux : le projet de loi qui nous est soumis, la loi de 1978 et le règlement européen. J'ajoute que la compréhension du dispositif sera complète lorsque nous disposerons de l'ordonnance, que le Gouvernement sera habilité à rédiger une fois le projet de loi adopté. Je regrette le recours à la procédure accélérée, mais nous sommes tenus par la date butoir du 25 mai. Il est d'ailleurs à remarquer que tous les pays européens, à part l'Allemagne et l'Autriche, qui ont déjà publié et voté leurs lois, sont dans la même démarche d'adaptation de leurs législations. J'ai effectué un certain nombre d'auditions, mais nous n'avons pas de visibilité complète sur la manière dont ces textes vont être transposés dans les différents États membres. Je ne peux donc pas répondre à toutes vos questions. La DG JUST continue pour sa part à faire des réunions d'information et de coordination entre pays pour essayer d'harmoniser au mieux. L'avantage d'avoir un texte large permet de continuer à le faire évoluer avec la jurisprudence, d'introduire des points de détails, des règlements, des recommandations de la CNIL qui peuvent couvrir des thèmes que vous avez mentionnés comme l'éducation au numérique. Au contraire, tout écrire et figer dans la loi, étant donné la vitesse à laquelle la technologie évolue, n'est pas forcément le meilleur choix.

Mme Marietta Karamanli. Le traitement des données en matière d'éducation et de scolarité est un sujet différent de l'éducation au numérique. Il est regrettable de ne pas avoir de régime spécifique pour ces données compte tenu de leur caractère sensible.

Mme Christine Hennion, rapporteure. Les données sont classifiées et ordonnées par le règlement. D'ailleurs, tout ce qui concerne les données de santé, les données génétiques et biométriques, est défini directement dans le règlement sans qu'il y ait à légiférer sur ce sujet. Les droits à l'oubli et à la portabilité ne sont pas mentionnés dans la loi parce que le RGPD est d'application directe pour cette matière. S'agissant du traitement des données sensibles, relevant de la sécurité et la défense nationale, cette question se trouve hors du champ du règlement et de la directive. Nous sommes encore en discussion avec les différents ministères : je poursuis mon travail d'audition avec la rapporteure au fond, Mme Paula Forteza, et la rapporteure pour avis, Albane Gaillot.

Au lieu d'avoir la CNIL qui délivre des autorisations au fur et à mesure, nous passons à un régime *a posteriori* ; c'est toute la philosophie de ce règlement, qui part du marché et vise à suivre au plus près ses évolutions. Les autorisations sont données souvent très tard : la réalité, c'est qu'un certain nombre d'entreprises sont coupées de la législation. Le choix qui a été effectué est de responsabiliser les entreprises : elles doivent apprendre ce que sont les données, elles vont devoir s'équiper de moyens, d'outils et avoir en interne ou en externe des spécialistes qui vont les aider sur ces questions, tels que les délégués à la protection des données. En revanche, les sanctions sont alourdies de manière à s'assurer que les entreprises jouent le jeu. C'est effectivement une révolution culturelle pour l'ensemble des acteurs, que ce soient les entreprises ou les administrations.

Madame la Présidente Sabine Thillaye. La décision de la Cour de Justice de mai 2014 « Google Spain » impose le droit à l'oubli, mais la machine, elle, n'oublie rien. Il faudrait parler plutôt d'autodétermination informationnelle. Les citoyens doivent dans ce domaine se responsabiliser en gérant au mieux la publicité de leurs données personnelles. Le législateur ne peut pas tout faire.

Mme Christine Hennion, rapporteure. J'encourage vivement la mise en place d'un système de médiation des données pour prévenir les conflits, en complément de l'action de la CNIL.

Mme Marietta Karamanli. Je regrette la lenteur de l'exécution des décisions. Des contenus interdits peuvent rester en ligne longtemps après la décision.

Mme Christine Hennion, rapporteure. Oui, et les moyens de la CNIL doivent être considérablement renforcés.

Puis, la Commission a autorisé la publication du rapport d'information.

ANNEXE N° 1 :
PRINCIPALES PROPOSITIONS

1. Porter à treize ans l'âge de consentement au traitement des données personnelles.

2. Encourager la création d'un système de certification et de labellisation européen pour les produits, les entreprises et les organismes qui respectent les dispositions du règlement.

3. Mettre en place un système de médiation dans une phase précontentieuse entre professionnels.

4. Prendre en compte, dans l'exercice de définition des études d'impact, les caractéristiques des entreprises innovantes et la difficulté de mesurer les risques dans le cadre d'activités en phase d'expérimentation.

5. Instaurer la possibilité de mettre en œuvre une action de groupe en responsabilité en cas de violation des dispositions du règlement et de la loi.

6. Encourager le Gouvernement, habilité par ordonnance par l'article 20 du projet de loi, à améliorer l'intelligibilité et la cohérence du texte pour assurer sa bonne application par les acteurs économiques.

ANNEXE N° 2 :
LISTE DES PERSONNES AUDITIONNÉES

Ministère de la Justice

– M. Eric Thiers, conseiller au cabinet en charge des questions constitutionnelles

– M. Anthony Duplan, chef du bureau du droit constitutionnel et du droit public général

– M. Corentin Hellendorff, rédacteur au bureau du droit constitutionnel et du droit public général

Ministère de l'Économie et des Finances - Direction générale de la concurrence, de la consommation et de la répression des fraudes

– Mme Marie-Christine Noiset, chef du bureau du groupe interministériel de la consommation et du conseil national de la consommation

– Mme Nicole Nespoulous, adjointe au chef du bureau du groupe interministériel de la consommation et du conseil national de la consommation

Médiation des entreprises

– M. Pierre Pelouzet, médiateur des entreprises

– M. Nicolas Mohr, directeur général

Commission européenne

– M. Emmanuel Crabit, directeur chargé des droits fondamentaux et de l'État de droit

– M. Olivier Micol, directeur chargé de la protection des données

– Mme Isabelle Chatelier

Qwant

– M. Léonard Cox, vice-président des affaires publiques et RSE

– M. Guillaume Champeau, directeur éthique et relations publiques

– M. Léonidas Kalogeropoulos, conseil

CIGREF

– M. Henri d'Agrain, délégué général

– Mme Flora Fischer, chargée de mission

UFC-Que Choisir

– Mme Justine Massera, juriste

– Mme Alice Jubeau, chargée de missions relations institutionnelles, responsable du lobbying européen

Entretiens menés par la rapporteure :

– M. Jean Lessi, secrétaire général de la CNIL

– Mme Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires de la CNIL

– M. Olivier Iteanu, avocat à la Cour

– Mme Nathalie Chiche, présidente de *Data Expert*, Médiateur, *Data Protection Officer* externe