N° 4544

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 22 février 2017.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE,

en conclusion des travaux d'une mission d'information [(1)]

sur les incidences des **nouvelles normes européennes** *en matière de* **protection** *des* **données personnelles** *sur la* **législation française**,

ET PRÉSENTÉ

PAR MME ANNE-YVONNE LE DAIN ET M. PHILIPPE GOSSELIN

Députés.

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

La mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française est composée de : Mme Anne-Yvonne Le Dain, *présidente et rapporteure* ; M. Philippe Gosselin, *vice-président- et co-rapporteur* ; Mme Cécile Untermaier, *vice-présidente ;* M. Luc Belot ; Mmes Colette Capdevielle ; Marie-Anne Chapdelaine ; Pascale Crozon ; M. Marc Dolez ; Mme Marietta Karamanli ; MM. Alain Tourret ; Patrice Verchère ; Mme Paola Zanetti ; M. Michel Zumkeller

SOMMAIRE

___

Pages

SYNTHÈSE DU RAPPORT

I. LE RÉGIME EN VIGUEUR DE LA PROTECTION DES DONNÉES PERSONNELLES : UN CADRE ANCIEN LAISSANT D'IMPORTANTES MARGES D'INTERPRÉTATION AUX ÉTATS MEMBRES

La directive 95/46/CE, en vigueur jusqu'au 25 mai 2018, a affirmé **les grands principes de la protection des données personnelles**, notamment en définissant ses concepts centraux et en fixant les conditions de licéité des traitements. Cependant, cette directive avait été élaborée dans le contexte des débuts d'internet, et n'a donc **pas pris en compte les évolutions technologiques majeures** intervenues du fait de son développement.

La Cour de justice de l'Union européenne a significativement contribué à préciser la définition du régime de protection des données personnelles, dans un sens particulièrement favorable aux droits des personnes.

En France, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés constitue, avant même la réglementation communautaire, un premier régime de protection des données personnelles des personnes physiques.

La marge de manœuvre laissée par la directive 95/46/CE a entraîné, en pratique, des différences dans les législations nationales. Au-delà de la volonté de certains États membres de diminuer les contraintes des responsables de traitement et de limiter la pression pesant sur les autorités nationales de contrôle, c'est également l'imprécision de certaines dispositions de la directive qui a permis de donner lieu à des applications variées.

II.– LE RÈGLEMENT DU 27 AVRIL 2016 : DES ÉVOLUTIONS SIGNIFICATIVES ET UN RENFORCEMENT VOLONTARISTE DE L'HARMONISATION DE LA PROTECTION DES DONNÉES PERSONNELLES

A. Le résultat d'une longue négociation

Le 25 janvier 2012, la Commission européenne a publié une proposition de règlement général sur la protection des données et une proposition de directive sur les données policières et judiciaires, ces deux textes constituant le « paquet données personnelles », qui a fait l'objet de plus de quatre ans de négociations.

De manière générale, la France a approuvé les objectifs d'approfondissement du cadre législatif de la directive 95/46/CE et de renforcement des droits des personnes concernées. Elle s'est opposée à toute disposition du règlement créant un recul par rapport au niveau de protection des droits des personnes assuré par cette directive.

Le texte final est le résultat d'un compromis, mêlant des dispositions harmonisées à de multiples renvois aux droits nationaux (une cinquantaine), ce qui en fait un règlement sui generis, laissant de nombreuses marges de manœuvre aux États membres. Ce résultat fait peser le risque d'une nouvelle fragmentation du régime de la protection des données personnelles dans l'Union européenne.

B. Le renforcement des droits des personnes physiques

Le règlement renforce les conditions applicables au **consentement** des personnes au traitement des données les concernant.

De nouveaux droits sont consacrés. Le **droit à l'oubli** recouvre le droit au déréférencement reconnu par la CJUE et un nouveau droit à l'effacement des données à caractère personnel. Le **droit à la portabilité** permet la récupération par les personnes concernées des données personnelles qu'elles ont fournies, dans un format réutilisable, ainsi que leur transmission à un autre responsable de traitement.

Le règlement précise également l'encadrement du **profilage**, c'est-à-dire des traitements de données personnelles visant à évaluer certains aspects personnels.

Les **actions collectives** en matière de protection des données personnelles sont autorisées. Les États membres pourront prévoir dans leur droit national que ces actions peuvent tendre à la réparation du préjudice subi.

C. Les principes s'imposant aux opérateurs traitant des données personnelles

● Le règlement « égalise » les obligations applicables aux sous-traitants et aux responsables de traitements, qui verront leur responsabilité conjointement engagée en cas de manquement à leurs obligations.

Par ailleurs, le champ d'application territorial du règlement est élargi. En pratique, le droit européen s'appliquera chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par internet.

● Alors que la directive de 1995 reposait en grande partie sur l'existence de formalités préalables (déclaration, autorisations), le règlement européen repose sur une **logique de conformité et de responsabilité**, dite d'« *accountability* ».

La responsabilisation des entreprises s'incarne par les **principes de la « protection des données dès la conception »** (*privacy by design*) et de **« protection des données par défaut »** (*privacy by default*), qui imposent aux responsables de traitement de mettre en œuvre toutes les techniques nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

Des **analyses de l'impact des traitements sur la protection des données à caractère personnel** devront être conduites par les responsables de traitement lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

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

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

● Le règlement donne aux autorités de contrôle la possibilité de prononcer des amendes administratives qui peuvent atteindre, selon la catégorie de l'infraction, **10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

● Les rapporteurs estiment qu'une attention particulière devra être accordée aux petites et moyennes entreprises qui pourront rencontrer des difficultés pour respecter les nouvelles obligations posées par le règlement.

D. L'encadrement des transferts de données à caractère personnel vers des pays tiers

Le règlement autorise les transferts de données fondés sur une décision de la Commission européenne constatant que le pays tiers assure un niveau de protection adéquat. Ces transferts seront également autorisés lorsque le responsable de traitement aura prévu des garanties telles que des règles d'entreprises contraignantes ou des clauses types de protection, ou dans certains cas limitativement énumérés (menace grave et immédiate pour la sécurité publique d'un État membre ou d'un État tiers, nécessité à des fins de prévention et de détection d'infractions pénales par exemple).

L'entrée en vigueur du règlement pose la question de son articulation avec l'accord « Bouclier vie privée » (*Privacy Shield*) que la Commission a conclu en février 2016 avec les États-Unis. Cet accord pourrait être remis en cause par la CJUE, qui en est saisie, ou par la Commission européenne elle-même, en raison du changement récent de politique des États-Unis en matière de protection des données personnelles.

E. Le renforcement des autorités de régulation et la mise en place d'un guichet unique

Le règlement implique une évolution des missions des autorités nationales de contrôle, qui auront un rôle essentiel d'accompagnement des responsables de traitement. Les amendes administratives qu'elles pourront prononcer seront considérablement renforcées.

Le nouveau mécanisme de décision conjointe de ces autorités, lorsqu'un traitement est transnational, représente également une évolution importante de leur mode de fonctionnement. En cas de désaccord entre ces autorités, un Comité européen de protection des données (CEPD) tranchera.

III. L'APPLICATION DU RÈGLEMENT À PARTIR DE MAI 2018 REND NÉCESSAIRE UNE ADAPTATION DU CADRE NATIONAL DE LA PROTECTION DES DONNÉES PERSONNELLES

L'interruption prochaine des travaux parlementaires imposera d'engager dès le début de la nouvelle législature la révision de la loi « Informatique et libertés » et **il est indispensable qu'un projet de loi puisse être déposé dès juin 2017.**

La **loi pour une République numérique** a pris en compte la problématique de la protection des données personnelles, sans pour autant couvrir l'ensemble du champ du règlement. Certaines de ses dispositions visent à anticiper l'application du règlement (droit à l'oubli numérique des mineurs), tandis que d'autres ont été adoptées à titre transitoire (renforcement des sanctions prononcées par la CNIL) ou traitent de sujets connexes (données des personnes décédées, portabilité des données n'ayant pas un caractère personnel).

A. De nécessaires adaptations

La loi devra adapter plusieurs dispositions relatives aux sanctions pouvant être prononcées par la CNIL. Si la loi pour une République numérique a d'ores et déjà prévu qu'à compter du 25 mai 2018, les sanctions entrant dans le champ du règlement seront celles prévues par ledit règlement, d'autres évolutions seront nécessaires concernant les mesures correctives ainsi que les sanctions d'autres manquements.

Par ailleurs, si le règlement prévoit les mécanismes de coopération et de décision des autorités nationales de contrôle, il ne comporte aucune disposition sur les règles procédurales, qui relèvent de la seule compétence des États membres. Les lignes directrices adoptées par le G 29 devraient donner un cadre au législateur.

B. Des questions restent en suspens

1. L'interprétation de certains concepts

Plusieurs notions évoquées dans le règlement devront être précisées par le G 29 afin de permettre une application uniforme du règlement parmi les États membres de l'Union européenne. C'est le cas par exemple de la notion de « risque élevé » nécessitant qu'un responsable de traitement consulte l'autorité de contrôle avant de mettre en œuvre un traitement de données.

Sur l'ensemble de ces notions, les rapporteurs considèrent que les avis du G 29 seront essentiels pour éviter toute incertitude juridique potentiellement préjudiciable pour les responsables de traitement et pour les personnes concernées.

2. Les règles spécifiques à certains types de traitements

Plusieurs dispositions du règlement prévoient que les États membres pourront maintenir ou adopter des règles spécifiques pour certains types de traitement.

S'agissant des données de santé, la question de la compatibilité avec le règlement européen du nouveau régime d'accès aux données de santé médico-administratives à caractère personnel défini par la loi de modernisation de notre système de santé du 26 janvier 2016 se posera lors de la discussion du projet de loi adaptant notre législation aux nouvelles normes européennes.

D'autres traitements font l'objet de règles spécifiques définies par la loi du 6 janvier 1978 : données biométriques et génétiques, traitements aux fins d'expression journalistique, artistique, et littéraire, traitements de données relatives aux infractions, aux condamnations et aux mesures de sûreté, traitements portant sur le numéro d'identification national, traitements à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques. Ces règles spécifiques devraient pouvoir être maintenues dans le cadre des marges ouvertes par le règlement.

3. Les actions de groupe

L'action de groupe, introduite par la loi du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle ( ), est ouverte lorsque plusieurs personnes physiques subissent un dommage ayant pour cause commune un manquement aux dispositions de la loi du 6 janvier 1978 et permet d'obtenir la cessation du manquement.

Le règlement prévoit la simple possibilité pour les États membres d'adopter des dispositions nationales autorisant des actions collectives avec mandat tendant à la réparation du préjudice subi. **La question d'un éventuel élargissement du champ de l'action de groupe devra donc être tranchée par le législateur.**

4. Le droit à la portabilité

La loi pour une République numérique prévoit la mise en œuvre, à compter du 25 mai 2018, d'un droit à la portabilité de l'ensemble de ses données pour le consommateur. S'agissant des données personnelles, elle renvoie au régime défini par l'article 20 du règlement. Les autres données relèvent d'un régime différent, ne s'imposant qu'aux opérateurs de communications électroniques.

Les rapporteurs estiment que la **mise en œuvre de ces deux régimes risque de poser des difficultés d'interprétation** et souhaitent que ceux-ci puissent être **clarifiés et mieux articulés dans le cadre de la future loi.**

5. Les dispositions spécifiques concernant les enfants

La question de l'articulation des dispositions nationales et du règlement se pose en raison **des âges différents fixés par la loi pour une République numérique (18 ans) et par le règlement (13 à 16 ans) pour l'exercice du droit à l'effacement** des données personnelles.

Cependant, selon une interprétation étudiée par le ministère de la justice, une disposition de l'article 17 du règlement, rendant obligatoire l'effacement des données pour respecter une obligation légale définie par le droit national, pourrait permettre de fixer une condition supplémentaire par rapport au règlement, telle que le prévoit la loi pour une République numérique s'agissant des mineurs âgés de 16 à 18 ans.

MESDAMES, MESSIEURS,

La directive du 24 octobre 1995 [1] a constitué une première étape dans l'élaboration à l'échelon européen d'un cadre juridique d'ensemble relatif à la protection des données personnelles. Compte tenu des évolutions du secteur et de la nécessité de renforcer la protection offerte en la matière, la Commission européenne a souhaité, dès 2012, rénover le cadre existant afin de l'adapter aux nouvelles réalités du numérique [2]. Après quatre ans de négociations, l'adoption du **règlement général sur la protection des données** [3], le 27 avril 2016, constitue l'aboutissement de cette volonté. Ce règlement a été complété par une directive sur les données policières et judiciaires [4], ces deux textes constituant le « paquet données personnelles ».

Comme l'a rappelé Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL) lors de son audition par la commission des Lois : « [le règlement européen] *inaugure une nouvelle ère dans la régulation puisqu'il consacre un changement de paradigme : il s'agit d'alléger considérablement ce que nous appelons les formalités préalables – les déclarations et autorisations – au profit d'une démarche de responsabilisation des acteurs et aussi d'un renforcement des droits des individus.* » [5]

Le règlement du 27 avril 2016 sera applicable à compter du 25 mai 2018, date à laquelle la directive 95/46 sera abrogée. Il est donc nécessaire d'adapter préalablement le cadre législatif de la protection des données à caractère personnel, principalement défini par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [6] qui constitue le socle juridique de la protection des données personnelles en France.

---

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

(2) Communication de la Commission européenne, « Protection de la vie privée dans un monde en réseau *», 25 mai 2012.*

(3) Règlement n° 2016/679 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.

(4) COM (2012) 10 final du 25 janvier 2012.

(5) Audition de Mme Isabelle Falque-Pierrotin, Assemblée Nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 12 octobre 2016.

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

La loi du 7 octobre 2016 pour une République numérique [(1)] a permis un renforcement significatif de la protection des données personnelles. Elle n'a pas cependant pas couvert l'ensemble du champ du règlement et une révision de la loi du 6 janvier 1978 est indispensable pour abroger les dispositions incompatibles ou redondantes – ce qui est l'effet classique d'un règlement – mais aussi pour adopter des dispositions nouvelles pour le compléter lorsqu'il ne peut s'appliquer directement.

L'interruption prochaine des travaux parlementaires jusqu'en juin 2017 imposera donc d'engager très rapidement ensuite la révision de la loi « Informatique et libertés » afin que les travaux législatifs aboutissent avant la fin de l'année 2017, compte tenu du temps nécessaire pour édicter les éventuels décrets d'application.

Dans la perspective du dépôt d'un projet de loi, la direction des affaires civiles et du sceau (DACS) du ministère de la Justice a mis en place un groupe de travail associant le commissaire du Gouvernement auprès de la CNIL, des agents de la DACS, des représentants de l'administration de la CNIL, des universitaires, ainsi que des agents de la direction des affaires criminelles et des grâces (DACG), chargée de la transposition de la directive sur les données policières et judiciaires. L'objectif est de parvenir à un projet de loi unique tirant les conséquences du règlement et transposant la directive. Le III de l'article 65 de la loi pour une République numérique prévoit que le Gouvernement remet au Parlement, **au plus tard le 30 juin 2017**, un rapport sur les modifications de la loi de 1978 rendues nécessaires par l'entrée en vigueur du règlement.

Compte tenu du calendrier précédemment évoqué, vos rapporteurs jugent indispensable que la transmission de ce rapport et le dépôt du projet de loi révisant la loi du 6 janvier 1978 soient concomitants et interviennent, dans les délais prévus, au mois de juin 2017.

Afin de préparer ces travaux législatifs, la commission des Lois a décidé, le 3 novembre 2016, la création d'une mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française et constitué une mission de treize membres afin que sur ce sujet d'importance, toutes les sensibilités politiques puissent être représentées.

Dans un calendrier particulièrement contraint [(2)], la mission a entendu les représentants de la CNIL, du secrétariat général des affaires européennes (SGAE), de la direction des affaires civiles et du sceau, de la direction interministérielle des systèmes d'information et de communication (DINSIC) et du Conseil national du numérique, des universitaires, des avocats, des associations représentant les usagers du Net (*la Quadrature du net,* l'association européenne des droits de

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

(2) Compte tenu de la fin prochaine des travaux de l'actuelle législature.

l'Homme) et les entreprises du numérique (association pour le commerce et les services en ligne), des entreprises (*Solocal group* et *Microsoft*) et des membres du cabinet de la secrétaire d'État chargée du numérique et de l'innovation. La mission a, par ailleurs, effectué un déplacement à Bruxelles durant lequel les rapporteurs ont notamment échangé avec les représentants de la direction générale chargée de la justice et des consommateurs de la Commission européenne et le contrôleur général de la protection des données.

Le premier enseignement de ces travaux est que **ce texte constitue un règlement *suis generis* à mi-chemin entre un règlement et une directive** et un compromis entre le droit romain et la *common law* (1).

En effet, le choix d'un règlement, directement applicable, plutôt qu'une directive témoigne de la volonté de disposer d'un régime juridique harmonisé dans l'ensemble de l'Union européenne. La marge de manœuvre laissée par la directive avait en effet entraîné, en pratique, de grandes différences dans les législations nationales.

Cependant ce texte est le fruit d'un compromis entre la volonté de la Commission de proposer un règlement d'application directe, afin de renforcer la cohérence de la protection des personnes et la volonté de certains États membres de pouvoir adapter certaines dispositions aux spécificités nationales. Il en résulte un texte qui mêle des dispositions harmonisées à de multiples renvois au droit national. Au total, le SGAE a ainsi comptabilisé **plus de cinquante dispositions**, de portée inégale, renvoyant au droit des États membres. La portée de l'harmonisation se trouve ainsi limitée par les nombreuses « clauses d'ouverture » figurant dans le texte final.

En second lieu, **ce texte constitue une véritable « révolution » en matière de protection des données personnelles** car il permet :

– le renforcement de la protection des données personnelles en reconnaissant **de nouveaux droits pour les personnes physiques**, – tels que le droit à l'effacement ou le droit à la portabilité des données ;

– **un champ d'application élargi** : le droit européen s'appliquera chaque fois qu'un résident européen, quelle que soit sa nationalité, sera directement visé par un traitement de données, y compris par internet et par le biais d'objets connectés ;

– **la responsabilisation des acteurs traitant les données,** en reconnaissant la responsabilité conjointe des responsables de traitement et des sous-traitants, et en adoptant à leur égard une logique de responsabilité. En contrepartie de la suppression de la plupart des obligations déclaratives, ces

(1) La principale différence entre les traditions juridiques de « common law *» et de droit civil repose sur la source principale du droit. Alors que les systèmes basés sur la «* common law *» considèrent les décisions judiciaires comme la source la plus importante de la loi, les systèmes basés sur le droit civil mettent particulièrement l'accent sur le droit codifié.*

derniers devront respecter un certain nombre d'obligations : tenir un registre des activités de traitement, conduire des analyses d'impact, désigner un délégué à la protection des données et notifier les violations de données à caractère personnel à l'autorité nationale de protection des données ;

– **le renforcement des autorités de régulation**, en leur permettant de prononcer des amendes administratives dont le montant est considérablement augmenté puisqu'elles pourront représenter, selon la catégorie de l'infraction – de 2 % à 4 % du chiffre d'affaires annuel mondial d'une entreprise, et de 10 à 20 millions d'euros pour les autres organismes – et en mettant en place un mécanisme de décision conjointe de l'ensemble des autorités de contrôle des États membres ;

– et **la création d'une instance européenne de coordination**, le Comité européen de protection des données (CEPD), véritable instance d'arbitrage européenne, qui favorisera la coordination des autorités de contrôle des États membres et l'émergence de pratiques communes en matière de protection des données personnelles. Malgré la mise en place de cette coopération européenne, le **mécanisme de « guichet unique »** garantira que, dans le cas de traitements transnationaux, les personnes concernées conserveront une proximité avec leur autorité de protection des données et leurs juridictions nationales, et que leur autorité de protection des données sera associée à la décision prise par l'autorité « chef de file ».

Enfin, ce règlement promeut l'affirmation d'une conception européenne de la protection des données personnelles, conception qui diffère de celle promue notamment par les États-Unis.

Comme l'ont rappelé plusieurs personnes entendues par la mission, cette conception, qui pourra paraître *a priori* contraignante pour les acteurs du numérique, constitue une opportunité de faire de l'Union européenne un espace où les entreprises, quelle que soit leur taille, pourront faire valoir la protection des données personnelles comme un avantage compétitif. Le règlement représente aussi une opportunité de développer certaines activités économiques, notamment dans l'accompagnement des entreprises qui devront respecter de nouvelles obligations. L'Union européenne représente un marché de consommateurs important dans le domaine du numérique : il ne s'agit donc pas seulement d'un enjeu de protections des données des résidents européens, mais également un enjeu économique et technologique.

Dans ce domaine, la France semble particulièrement bien « armée » car elle peut faire valoir une culture de la protection des données et une véritable expertise juridique dans ce domaine, comme en témoigne son rôle important lors des négociations sur le règlement. Par ailleurs, vos rapporteurs estiment que le règlement est aussi une opportunité pour la France de développer des compétences en ces domaines sur tout le territoire national, l'économie numérique pouvant par nature être très décentralisée.

Cependant cette différence de conception entre les États-Unis et l'Union européenne n'est pas sans conséquence sur les transferts de données des usagers européens vers les entreprises américaines. Dans un arrêt du 6 octobre 2015 [1], la Cour de justice de l'Union européenne (CJUE) a invalidé de la décision n° 2000/520/CE de la Commission constatant que les États-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées et permettant l'application de l'accord conclu entre les États-Unis et l'Union européenne appelé « Sphère de sécurité » (« *Safe Harbor* »). À la suite de cet arrêt, la Commission a conclu en février 2016 un nouvel accord avec les États-Unis sur le cadre des transferts transatlantiques de données, le « bouclier vie privée Union européenne-États-Unis » (EU-US *Privacy shield*).

Or, bien que la décision d'exécution de la Commission européenne du *Privacy Shield* intègre par anticipation certaines des avancées prévues par le règlement, la pérennité de cet accord pourrait être remise en cause dans les mois qui viennent, compte tenu de certaines réserves émises par le groupe qui rassemble les autorités de contrôle des États membres de l'article (G29) sur celui-ci, du recours déposé par plusieurs associations contre cet accord devant la Cour de justice de l'Union européenne et de la remise en cause, par le Président Donald Trump – notamment par le décret adopté le 25 janvier 2017 –, des garanties accordées aux citoyens de l'Union européenne en matière de protection des données personnelles sous la présidence de Barack Obama [2]. Le 15 février, le G29 a indiqué, dans un communiqué, qu'une lettre serait envoyée aux autorités américaines faisant état de ses inquiétudes et demandant une clarification sur l'impact du décret du président des États-Unis sur le *Privacy Shield*.

En France, si certaines mesures d'adaptation requises par le règlement ne suscitent pas de débats, **d'autres questions demeurent en suspens et devront être tranchées par le législateur**. C'est le cas notamment des règles spécifiques à certains traitements de données – en matière de santé ou biométriques par exemple , de celles relatives aux actions de groupe, au droit à la portabilité ou des dispositions spécifiques applicables aux mineurs.

Les travaux conduits par la mission lui ont permis de prendre la mesure du chantier législatif qui s'annonce et qui devra être ouvert dès le début de la prochaine législature afin qu'un texte définitif puisse être adopté afin la fin de l'année 2017.

*

* *

(1) CJUE, 6 octobre 2015, C-362/14, Schrems.

(2) Comme en témoigne le décret adopté le 25 janvier 2017

I. LE RÉGIME EN VIGUEUR DE LA PROTECTION DES DONNÉES PERSONNELLES DANS L'UNION EUROPÉENNE : UN CADRE ANCIEN LAISSANT D'IMPORTANTES MARGES D'INTERPRÉTATION AUX ÉTATS MEMBRES

La directive 95/46/CE du 24 octobre 1995, applicable jusqu'au 25 mai 2018, constitue le cadre de référence de la protection des données dans l'Union européenne.

Cette directive n'est pas le premier instrument juridique de protection des données personnelles en Europe. Dès 1981, le Conseil de l'Europe a en effet adopté une convention pour la protection des personnes à l'égard des traitements automatisés des données à caractère personnel, **la convention 108**, aujourd'hui ratifiée par l'ensemble de ses États membres. Cette convention pose les principes de la collecte licite et loyale des données, de leur traitement à des fins légitimes définies, de leur caractère exact et non excessif par rapport aux finalités du traitement, ainsi que de leur conservation pendant une durée n'excédant pas celle nécessaire à ces finalités. Elle reconnaît le droit pour toute personne physique d'être informée de l'existence du traitement et de rectifier ses données. Elle autorise également les États parties à limiter les transferts internationaux de certaines catégories de données personnelles vers des États tiers lorsqu'ils ne garantissent pas une protection équivalente.

Par ailleurs, le droit à la protection des données personnelles fait partie des droits protégés par **l'article 8 de la Convention européenne des droits de l'homme**, dans le cadre du droit au respect de la vie privée et familiale, du domicile et de la correspondance.

A. LE CADRE DE RÉFÉRENCE DÉFINI PAR LA DIRECTIVE DE 1995, COMPLÉTÉ PAR LA DIRECTIVE DE 2002 « VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES »

1. La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

a. L'affirmation des grands principes de la protection des données personnelles

L'adoption de la directive 95/46/CE du 24 octobre 1995 a été la première étape de l'élaboration d'un cadre juridique européen relatif à la protection des données personnelles.

La directive ne s'applique pas au traitement des données à caractère personnel transmises ou mises à disposition entre les États membres dans le cadre

de la coopération judiciaire en matière pénale et de la coopération policière, qui relève d'une décision-cadre de 2008 [(1)].

L'article 2 de la directive définit plusieurs concepts centraux pour la protection des données personnelles.

Les données à caractère personnel sont définies comme « *toute information concernant une personne physique identifiée ou identifiable* […] *; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».

Ces informations peuvent être nominatives ou non. L'image d'une personne ou d'éléments se rapportant à cette personne est une donnée à caractère personnel si elle permet d'identifier la personne. Les personnes dont l'image apparaît dans des applications telles que *Google Street View* ont donc le droit d'obtenir le floutage de cette image au titre de la protection de leurs données personnelles.

Le traitement de données à caractère personnel désigne « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ».

Le responsable de traitement de données personnelles est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire* ».

Le sous-traitant est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

---

(1) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Ce texte relève de l'ancien « troisième pilier » de l'Union européenne relatif à la justice et aux affaires intérieures.

Les responsables du traitement de données et leurs sous-traitants doivent respecter différents principes en matière de protection des libertés individuelles et des données à caractère personnel.

En application de l'article 6, les données à caractère personnel doivent être traitées **loyalement et licitement**, collectées pour **des finalités déterminées**, **explicites et légitimes**. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, exactes et, si nécessaire, mises à jour. Elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

L'article 7 définit les **conditions de licéité du traitement**. Celui-ci ne peut être effectué que dans les cas suivants :

– la personne concernée a **indubitablement donné son consentement** ;

– le traitement est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ;

– le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;

– le traitement est nécessaire à la **sauvegarde de l'intérêt vital** de la personne, ou à **l'exécution des missions d'intérêt public** relevant de l'exercice de l'autorité publique ;

– le traitement est nécessaire à la **réalisation de l'intérêt légitime poursuivi par le responsable du traitement**, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le groupe de l'article 29 (G29), qui rassemble les autorités de contrôle des États membres, a adopté en 2014 un avis précisant l'interprétation de cette condition [(1)].

L'article 8 **interdit en principe le traitement des données dites sensibles**, c'est-à-dire celles qui peuvent révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la santé et à la vie sexuelle. Il prévoit néanmoins plusieurs exceptions : consentement de la personne, respect des obligations et droits du responsable de traitement en matière de droit du travail, défense des intérêts vitaux de la personne, activités de certains organismes à but non lucratif, données rendues publiques ou nécessaires à l'exercice d'un droit en justice, domaine médical.

En application de l'article 10, le responsable du traitement doit fournir des informations à la personne auprès de laquelle il collecte les données. Ces informations sont relatives à l'identité du responsable du traitement, aux finalités

(1) Groupe de l'article 29, avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avril 2014, 844/14/FR ,WP 21.

du traitement, aux destinataires des données, au caractère facultatif ou non de la réponse aux questions posées et au droit d'accès aux données.

La personne dont les données sont soumises à un traitement dispose d'un **droit d'accès** à ces données qui doit être possible sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs ; elle doit pouvoir obtenir leur rectification, leur effacement ou leur verrouillage si leur traitement n'est pas conforme à la directive (article 12). Elle doit également pouvoir s'opposer au traitement, au moins lorsqu'il est fondé sur un intérêt public ou sur l'intérêt légitime du responsable de traitement, pour des raisons prépondérantes et légitimes tenant à sa situation particulière. Elle peut également s'opposer à tout traitement à des fins de prospection (article 14). La directive n'impose pas de forme particulière pour l'exercice de ces droits, ce qui peut poser la question de la facilité avec laquelle la personne peut, ou non, les exercer.

En application de l'article 18, les responsables du traitement de données et leurs sous-traitants doivent respecter une **obligation de notification à l'autorité de contrôle** de la protection des données, la Commission nationale de l'informatique et des libertés (CNIL) en France, préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé de données à caractère personnel. Ces notifications sont obligatoires et ne peuvent faire l'objet de dérogation que dans des conditions limitativement énumérées. Par ailleurs, ceux des traitements de données susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes physiques sont soumis à un régime plus strict et doivent faire l'objet d'un examen avant leur mise en œuvre.

L'article 28 prévoit que chaque État membre dispose d'une ou plusieurs autorités publiques indépendantes chargées de surveiller le respect, sur son territoire, des dispositions adoptées par les États membres en application de la directive. Ces autorités sont rassemblées au sein d'un groupe de protection des personnes en matière de traitement de données à caractère personnel, en application de l'article 29.

b. Des limites liées à l'évolution de l'environnement numérique et aux divergences d'application dans les États membres

La directive 95/46 avait été élaborée dans le contexte des débuts d'internet, et n'avait donc pas pris en compte les évolutions technologiques majeures intervenues du fait de son développement. La directive de 2002 sur la vie privée et les communications électroniques [(1)] a eu pour objectif de combler certaines lacunes du cadre juridique mais la massification du partage, de la

(1) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; cette directive s'est substituée à la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

collecte et du traitement des données personnelles, ainsi que la facilité d'usage et le confort d'utilisation des nouveaux services offerts par internet ont fait apparaître de nouveaux enjeux de protection des droits fondamentaux.

Ainsi, M. Edouard Geffray, secrétaire général de la CNIL, a estimé lors de son audition par la mission d'information, que la directive 95/46, tout en reposant sur des principes solides et pertinents (légitimité du traitement, finalités, proportionnalité, droits des personnes), ne correspondait plus, sur plusieurs points, à l'évolution du monde numérique :

– son **champ d'application territorial**, fondé sur le lieu d'implantation du responsable de traitement, et non sur le lieu de résidence des personnes concernées par les traitements, limite sa portée en termes de protection, dans un environnement fortement dématérialisé et très internationalisé, alors même que des pays non européens se sont dotés d'instruments juridiques puissants ;

– son **champ d'application personnel** se limite aux responsables de traitement, c'est-à-dire aux donneurs d'ordre, sans prendre en compte les sous-traitants, alors que le recours à la sous-traitance est très fréquent dans le domaine du traitement des données personnelles car ce sont souvent ces acteurs qui maîtrisent les technologies, ainsi que les accès et les usages des réseaux ;

– le **régime de contrôle** actuel, qui s'est construit historiquement sur « *le diptyque formalités préalables/contrôle a posteriori* » ne correspond plus à l'évolution des techniques et des usages, le régime de déclaration ayant perdu sa pertinence ; les autorités de contrôle doivent désormais accompagner la mise en conformité des entités concernées afin qu'elles assurent une protection optimale des données personnelles à chaque instant

En outre, la directive, qui laisse de vastes marges d'interprétation aux États membres, a donné lieu à des transpositions nationales diverses. Ainsi que le relève le considérant (9) du règlement du 27 avril 2016, « *la directive 95/46/CE n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique ou le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne. Les différences dans le niveau de protection des droits et libertés des personnes physiques, en particulier le droit à la protection des données à caractère personnel* [...] *peuvent empêcher le libre flux de ces données dans l'ensemble de l'Union. Ces différences peuvent dès lors constituer un obstacle à l'exercice des activités économiques au niveau de l'Union, fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union. Ces différences dans le niveau de protection résultent de l'existence de divergences dans la mise en œuvre et l'application de la directive 95/46/CE.* »

2. La directive 2002/58/CE du 12 juillet 2002 « vie privée et communications électroniques »

La directive 2002/58/CE du 12 juillet 2002 « vie privée et communications électroniques » traduit dans le secteur des services de communication électronique les principes définis par la directive 95/46. Elle concerne en outre la protection des intérêts légitimes des personnes morales dans ce secteur.

La directive impose aux fournisseurs de services de communication électronique de prendre les mesures appropriées pour garantir la **sécurité de leurs services**. En cas de violation de la sécurité des données personnelles, ils doivent informer l'autorité nationale de contrôle et, dans certains cas, l'abonné.

Les États membres doivent garantir dans leur législation **la confidentialité des communications** et des données de trafic y afférentes. Ils doivent en particulier interdire à toute personne autre que les utilisateurs l'écoute, l'interception, le stockage des communications et des données relatives au trafic y afférentes, ou l'utilisation de tout autre moyen d'interception ou de surveillance sans le consentement des utilisateurs concernés, sauf lorsque la personne y est légalement autorisée.

La portée des droits et des obligations énoncés par la directive ne peut être limitée par des mesures législatives nationales que de manière nécessaire et proportionnée pour sauvegarder la sécurité nationale, la défense ou la sécurité publique ou dans le cadre d'enquêtes pénales.

Le stockage des informations ou l'accès à des informations stockées dans l'équipement terminal d'un utilisateur (« **cookies** ») [(1)] n'est autorisé que si celui-ci est informé de manière claire et complète, entre autres des finalités du traitement, et s'il a le droit de refuser un tel traitement.

Le traitement des **données de localisation**, n'est autorisé que si celles-ci ont été rendues anonymes ou si l'utilisateur y a consenti, « *dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée* ».

Le consentement des utilisateurs est également requis pour l'envoi de communications non sollicitées (prospection par SMS ou par messagerie électronique). Les abonnés doivent pouvoir décider de figurer dans un annuaire public et la non-inscription doit être gratuite. Enfin, les utilisateurs doivent pouvoir refuser l'identification de leur numéro lorsqu'ils émettent un appel.

---

(1) Les « cookies » sont des fichiers déposés dans le terminal d'un utilisateur, par exemple lors de la consultation d'un site internet, afin, notamment, d'enregistrer des informations sur cet utilisateur.

B. L'APPORT DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE AU RÉGIME EUROPÉEN DE PROTECTION DES DONNÉES PERSONNELLES

La Cour de justice de l'Union européenne (CJUE) a significativement contribué à préciser la définition du régime de protection des données personnelles, **dans un sens particulièrement favorable aux droits des personnes**.

Par sa décision du 13 mai 2014, *Google c/Espagne* [(1)], la Cour a considéré que l'exploitant d'un moteur de recherche sur internet pouvait être tenu de supprimer des listes de résultats de recherche ceux permettant de relier le nom d'une personne à des pages web, lorsque celles-ci sont porteuses d'une violation des données personnelles de l'individu. La Cour a ainsi consacré un droit au « déréférencement » [(2)].

Par ailleurs, dans une décision du 8 avril 2014 [(3)], la Cour de justice a invalidé la directive n° 2006/24/CE relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication. Cette directive, qui modifiait la directive 2002/58/CE, avait fait l'objet de réserves sérieuses exprimées par le G29 [(4)]. La Cour a invalidé la directive au motif qu'elle conduisait à une ingérence disproportionnée dans les droits fondamentaux des individus en matière de données personnelles.

Ladite directive autorisait en effet une conservation des données personnelles, dérogatoire au régime de protection des données déterminé par les directives n° 95/46 et n° 2002/58/CE justifiée, selon la Commission, par la lutte contre la criminalité mais invalide au regard de la Charte des droits fondamentaux de l'Union Européenne, selon la Cour.

Enfin, dans un arrêt du 6 octobre 2015, dit *Schrems*, la Cour de justice a invalidé la décision n° 2000/520/CE de la Commission constatant que les États-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées et permettait l'application de l'accord conclu entre les États-Unis et l'Union européenne appelé « Sphère de Sécurité » (« *Safe Harbor* »). Cette décision de la Commission, qui rendait possible le transfert de données personnelles entre entreprises de l'Union européenne et entreprises américaines, a été invalidée par la Cour au motif que ce pays ne présentait pas des garanties suffisantes en matière de protection des données personnelles [(5)].

---

(1) CJUE, 13 mai 2014, C-131/12, Google c/Espagne.

(2) Elle a aussi considéré que l'exploitant d'un moteur de recherche sur internet était « responsable d'un traitement de données personnelles *» [(2)], au sens de la directive 95/46/CE, lorsqu'il indexe et met à disposition des données personnelles figurant sur des pages web publiées par des tiers.*

(3) CJUE, 8 avril 2014, affaires jointes n° C-293/12 et C-594/12.

(4) https://www.cnil.fr/fr/la-directive-200624ce-contraire-aux-articles-7-et-8-de-la-charte-des-droits-fondamentaux-de-lunion.

(5) CJUE, 6 octobre 2015, C-362/14, Schrems.

L'accord sur la Sphère de Sécurité posait un ensemble de principes de protection des données personnelles, auquel les entreprises établies aux États-Unis pouvaient volontairement adhérer afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union Européenne. La Cour de justice a estimé que ce dispositif, qui visait à compenser l'insuffisance de la législation américaine en matière de protection des données personnelles par rapport à la législation européenne, ne présentait pas des garanties suffisantes du fait des ingérences possibles des autorités publiques américaines dans les données personnelles ainsi transmises (1) et qu'il violait les droits garantis par la Charte européenne des droits fondamentaux.

À la suite de l'arrêt *Schrems*, la Commission a conclu en février 2016 un nouvel accord avec les États-Unis sur le cadre des transferts transatlantiques de données, le « bouclier vie privée Union européenne-États-Unis ». (2)

C. LES MESURES NATIONALES DE PROTECTION DES DONNÉES PERSONNELLES DES PERSONNES PHYSIQUES

Les États membres ont adopté des mesures nationales afin d'assurer la mise en œuvre des principes fixés par l'Union européenne et assurer la protection des données personnelles.

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (3) constitue, avant même la réglementation communautaire, un premier régime de protection des données personnelles des personnes physiques en France. Elle a été modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (4) transposant la directive 95/46/CE, qui n'avait pas encore été transposée en droit interne (5), et la directive 2002/58/CE. Elle institue notamment la Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante dont la mission est de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi (2° de l'article 11 de la loi). La loi encadre à ce titre les traitements automatisés et non automatisés de données personnelles (article 2 alinéa 1er de la loi).

La marge de manœuvre laissée par la directive a entraîné, en pratique, des différences dans les législations nationales.

---

(1) Ces insuffisances ont notamment été mises en lumières par les révélations de M. Edward Snowden sur la surveillance pratiquée par l'Agence nationale de la sécurité (NSA), voire par l'espionnage du téléphone portable de Mme Merkel par cette agence.

(2) Cf. infra.

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

(4) 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.

(5) La directive 95/46/CE a été transposée tardivement par la loi du 6 août 2004 relative à la protection des personnes physiques concernant les traitements de données à caractère personnel.

Par exemple, dans les limites posées par la directive 95/46, le législateur suédois a nettement allégé les obligations déclaratives s'imposant aux opérateurs assurant un traitement de données personnelles auprès de la *Datainspektion* (équivalent suédois de la CNIL). Les formalités déclaratives s'imposant aux opérateurs économiques sont ainsi moindres que celles applicables à un État membre tel que la France (en 2006, seulement 215 déclarations préalables sont réalisées à la *Datainspektion* contre 72 000 pour la CNIL [(1)]). Par ailleurs, la législation suédoise a exonéré les traitements courants de données personnelles de la plupart des règles matérielles entourant l'utilisation desdites données.

Au-delà de la volonté de certains États membres de **diminuer les contraintes** des opérateurs traitant des données personnelles et **de limiter la pression pesant sur les autorités nationales de contrôle**, c'est également **l'imprécision de certaines dispositions** de la directive 95/46 qui a permis de donner lieu à des applications variées, comme dans le cas des formalités administratives (articles 18 et suivants de la directive) qui a fait l'objet d'une application différente en France et en Suède.

II. LE RÈGLEMENT DU 27 AVRIL 2016 : DES ÉVOLUTIONS SIGNIFICATIVES ET UN RENFORCEMENT VOLONTARISTE DE L'HARMONISATION DE LA PROTECTION DES DONNÉES PERSONNELLES DANS L'UNION EUROPÉENNE

A. LE RÉSULTAT D'UNE LONGUE NÉGOCIATION

1. Le paquet « données personnelles »

La Commission européenne a lancé dès 2009, à travers une consultation publique, une réflexion sur la nécessité de réexaminer le cadre juridique de la protection des données personnelles, compte tenu des évolutions technologiques rapides et de la mondialisation. En novembre 2010, elle a publié une communication fixant les objectifs essentiels d'une nouvelle approche globale de la protection des données personnelles, dans laquelle elle annonçait son intention de présenter des propositions législatives [(2)].

Ce processus s'est inscrit dans le contexte de **l'évolution du cadre institutionnel de la protection des données personnelles**. En raison de l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, l'article 8 de la Charte des droits fondamentaux de l'Union européenne, relatif à la protection des données personnelles, a acquis une force juridiquement contraignante. En outre, l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui reconnaît

---

(1) Patricia Blanc-Gonnet Jonason, « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle *», 2008, AJDA.*

(2) 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.*

également le droit à la protection des données personnelles, a créé une base juridique propre à cette protection [1].

Article 8 de la Charte des droits fondamentaux de l'Union européenne

« 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. »

Article 16 du traité sur le fonctionnement de l'Union européenne

« 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. »

Le 25 janvier 2012, la Commission européenne a publié une proposition de règlement général sur la protection des données [2] et une proposition de directive sur les données policières et judiciaires [3], ces deux textes constituant le « paquet données personnelles ».

Compte tenu des délais restreints dans lesquels la mission d'information a mené ses travaux, vos rapporteurs ont fait le choix d'analyser en priorité l'impact du règlement, qui constitue le futur cadre général de la protection des données personnelles. L'encadré ci-dessous ne constitue donc qu'une présentation synthétique des grandes lignes de la directive adoptée le même jour.

(1) La directive 95/46 se fondait sur l'article 100A du traité instituant la Communauté européenne (TCE), relatif au marché intérieur.

(2) COM (2012) 11 final du 25 janvier 2012.

(3) COM (2012) 10 final du 25 janvier 2012.

La directive 2016/ 680 du 27 avril 2016 relative à la protection des données personnelles en matière policière et judiciaire [(1)]

Alors que la décision-cadre de 2008 ne visait que les échanges de données entre États membres ou entre États membres et États tiers, la directive relative à la protection des données personnelles en matière policière et judiciaire s'applique aux traitements de données effectués par les autorités compétentes au sein des États membres en matière de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales.

La directive applique aux données personnelles en matière policière et judiciaire les grands principes de la protection des données personnelles : les données devront être traitées de manière licite et loyale ; collectées pour des finalités déterminées, adéquates, pertinentes et non excessives par rapport aux finalités du traitement ; exactes et, si nécessaire, mises à jour ; conservées sous une forme permettant l'identification des personnes pendant une durée n'excédant pas celle nécessaire au regard des finalités.

Les personnes concernées par le traitement de leurs données personnelles disposeront d'un droit à l'information, portant notamment sur l'identité et les coordonnées du responsable du traitement, les finalités du traitement, l'existence du droit d'accès et d'un droit de réclamation auprès de l'autorité de contrôle.

Un droit d'accès des citoyens aux données les concernant ainsi qu'à certaines informations est également prévu. Toutefois, les États membres pourront, par la loi, limiter ce droit d'accès, si cette limitation « *constitue une mesure nécessaire et proportionnée dans une société démocratique* », compte tenu des intérêts légitimes de la personne (pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, éviter de nuire à la poursuite d'infractions pénales, protéger la sécurité publique et la sûreté de l'État, protéger les droits et libertés d'autrui).

Enfin, un droit à la rectification des données inexactes et à l'effacement des données dont le traitement est illicite s'exercera directement auprès du responsable du traitement.

Les responsables de traitement devront mettre en œuvre les principes de protection des données dès la conception et par défaut [(2)]. Ils devront fournir une analyse de l'impact du traitement sur la protection des données personnelles lorsque ce traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Ils devront également notifier les violations de données à l'autorité de contrôle, ainsi qu'aux personnes concernées en cas de risque élevé pour leurs droits et libertés.

Les transferts de données vers des pays tiers ne pourront avoir lieu que s'ils sont nécessaires à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite, ou d'exécution de sanctions pénales.

---

(1) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

(2) Cf. infra.

Ces transferts seront autorisés lorsque la Commission européenne aura adopté une décision constatant le caractère adéquat du niveau de protection dans l'État tiers. En l'absence d'une telle décision, le transfert pourra avoir lieu lorsqu'il existe des « *garanties appropriées* », qui devront être offertes par un instrument juridiquement contraignant, tel qu'une convention internationale, ou dans certains cas limitativement énumérés (menace grave et immédiate pour la sécurité publique d'un État membre ou d'un État tiers, nécessité à des fins de prévention et de détection d'infractions pénales par exemple).

La directive doit être transposée par les États membres avant le 6 mai 2018.

Les discussions sur le paquet « données personnelles » ont duré plus de quatre ans, ce qui représente une durée exceptionnellement longue. Ainsi que l'a indiqué Mme Aurélia Schaff, chef du secteur « espace judiciaire européen » au secrétariat général des affaires européennes (SGAE) devant la mission d'information, cette durée s'explique certes par la technicité du sujet mais aussi par les fortes réticences de nombreux États membres. Les négociations ont été particulièrement laborieuses s'agissant du règlement, qui compte au final 99 articles et 173 considérants. Ce n'est qu'en juin 2014 qu'ont pu être dégagés de premiers accords partiels au Conseil, une année supplémentaire ayant ensuite été nécessaire pour examiner l'ensemble du texte. Le Parlement européen avait pour sa part adopté sa position en première lecture en mars 2014. Le trilogue entre le Conseil, le Parlement européen et la Commission européenne s'est ensuite déroulé plus rapidement.

2. La position de la France

Les grandes lignes de la position défendue par les autorités françaises sur la proposition de règlement ont été exposées par Mme Aurélia Schaff lors de son audition ainsi que dans ses réponses écrites au questionnaire des rapporteurs.

De manière générale, la France a approuvé les objectifs d'approfondissement du cadre législatif de la directive 95/46 et de renforcement des droits des personnes concernées. Elle s'est **opposée à toute disposition du règlement créant un recul** par rapport au niveau de protection des droits des personnes assuré par cette directive.

Elle s'est notamment montrée **défavorable à l'établissement d'une catégorie distincte de données à caractère personnel pour les données pseudonymisées**, défendue par certains États membres, dont l'Allemagne. Dans cette hypothèse, la pseudomynisation aurait permis au responsable de traitement de se soustraire au respect de certaines obligations du règlement. Les autorités françaises ont estimé qu'une telle disposition affaiblirait les droits des personnes, la pseudonymisation ne présentant pas les mêmes garanties de protection que l'anonymisation, et qu'elle ne permettrait pas d'assurer la neutralité technologique du règlement. Le texte adopté a répondu à ces préoccupations puisque les données pseudonymisées restent définies comme des données à caractère personnel.

La pseudonymisation des données à caractère personnel

L'article 4 du règlement du 27 avril 2016 définit la pseudonymisation comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

La pseudonymisation consiste à remplacer certaines données personnelles par un pseudonyme, par exemple grâce à un cryptage des données avec une clé secrète. La ré-identification de la personne demeure possible au moyen de la clé.

Le considérant 26 précise que « *les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable*. »

Le considérant 28 cite la pseudonymisation comme un moyen de réduire les risques pour les personnes concernées, tout en précisant qu'il peut être recouru à d'autres techniques de protection des données.

La pseudonymisation est **distincte de l'anonymisation**, qui est « *le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification* » [(1)]. Les données anonymisées ne sont pas considérées comme des données personnelles et sont donc situées hors du champ du règlement.

Selon le considérant 26 du règlement, « *pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci*. »

En raison de la spécificité des missions d'intérêt public et de contrôle des autorités publiques, la France s'est opposée à ce que les traitements de données par ces autorités soient soumis à des règles plus strictes et plus contraignantes que les traitements de données par le secteur privé.

Elle a soutenu le processus de **responsabilisation des entreprises et l'approche fondée sur les risques**. Elle a également promu le recours aux **actions de groupe** devant les juridictions et les autorités de contrôle, le renforcement du montant des **sanctions encourues**, l'introduction de dispositions encadrant le traitement des **données des personnes décédées**, la facilitation de **l'exercice du**

(1) G29, avis 05/2014 sur les Techniques d'anonymisation adopté le 10 avril 2014, 0829/14/FR-WP216.

« droit à l'oubli » pour les personnes mineures au moment de la collecte de leurs données.

Dans la proposition de règlement initiale, le critère de l'établissement principal du responsable de traitement déterminait l'autorité nationale de contrôle compétente. La France, fortement soutenue par l'Allemagne, a souhaité que le **mécanisme de « guichet unique »** garantisse que, dans le cas de traitements transnationaux, les personnes concernées conservent une proximité avec leur autorité de protection des données et leurs juridictions nationales, et que leur autorité de protection des données soit associée à la décision prise par l'autorité « chef de file ». Elle a également souhaité que le nouveau mécanisme assure une prise de décision collective et mise en œuvre de façon uniforme sur le territoire européen, en associant toutes les autorités de protection des données concernées et en conférant au comité européen de la protection des données créé par le règlement , doté de la personnalité juridique, le pouvoir d'adopter des décisions contraignantes pour régler les différends éventuels entre autorités de contrôle nationales.

Enfin, la France s'est montrée favorable, comme l'Allemagne, à un encadrement plus strict des transferts internationaux de données personnelles lorsqu'ils étaient opérés à la demande d'autorités publiques des États tiers.

En application de l'article 88-4 de la Constitution, **l'Assemblée nationale s'est prononcée dès 2012 sur la proposition de règlement par une résolution européenne, proposée par votre co-rapporteur** (1).

Elle avait alors exprimé son soutien à l'introduction des nouveaux droits prévus dans la proposition de règlement (« droit à l'oubli », « droit à la portabilité ») (2) ainsi qu'au renforcement des règles relatives au consentement. Elle s'était prononcée contre le critère de l'établissement principal du responsable de traitement et avait défendu le maintien de la compétence de l'autorité de protection d'un État sur tout traitement de données ciblant spécifiquement la population de cet État. Elle avait également souligné la nécessité de renforcer l'encadrement des transferts internationaux de données.

Les négociations sur le paquet « données personnelles » ont ensuite fait l'objet d'un suivi, tant au sein de la commission des affaires européennes que de la commission des Lois (3).

---

(1) Cf. annexe 2, résolution européenne sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, texte adopté n°888 du 23 mars 2012 ; rapport de la commission des affaires européennes n° 4227 du 7 février 2012 présenté par M. Philippe Gosselin.

(2) Cf. infra.

(3) Communication de M. Guy Geoffroy et de Mme Marietta Karamanli, commission des Lois, 17 octobre 2012, compte-rendu n° 4 ; communication de M. Guy Geoffroy, commission des Lois, 11 juin 2014, compte-rendu n° 64 ; communication de M. Guy Geoffroy, commission des affaires européennes, 15 février 2012, compte-rendu n° 241 ; communication de Mme Marietta Karamanli, commission des affaires européennes, 14 mai 2014.

3. Un règlement *sui generis*, laissant d'importantes marges de manœuvre aux États membres

La Commission européenne a fait le choix de proposer un règlement, d'application directe, pour remplacer la directive de 95/46, qui avait dû faire l'objet de mesures de transposition nationales. Elle a ainsi souhaité renforcer la cohérence de la protection des personnes, la sécurité juridique ainsi que la libre circulation des données à caractère personnel au sein du marché intérieur, en évitant les divergences de transposition.

Cependant, certains États membres auraient souhaité maintenir une directive, instrument plus souple, et le règlement final est le résultat d'un compromis, mêlant des dispositions harmonisées à de multiples renvois au droit national. Au total, le SGAE a ainsi **comptabilisé plus de cinquante dispositions, de portée inégale, renvoyant au droit des États membres**. La liste de ces dispositions, communiquée à vos rapporteurs, est publiée en annexe du présent rapport [(1)].

La portée de l'harmonisation se trouve ainsi limitée par les nombreuses « clauses d'ouverture » figurant dans le texte final, qui diffère à cet égard d'un règlement classique.

Les renvois au droit national peuvent être obligatoires :

– l'article 51 prévoit ainsi que chaque État membre définit le statut de l'autorité de contrôle chargée de veiller à l'application du règlement ;

– l'article 84 dispose que les États membres déterminent le régime des sanctions que le règlement n'a pas harmonisées.

Ces renvois constituent cependant la plupart du temps une faculté laissée aux États membres, par exemple :

– pour adapter l'application du règlement s'agissant des traitements nécessaires à l'exécution d'une mission d'intérêt public (article 6, paragraphes 2 et 3) ;

– pour fixer l'âge en dessous duquel le consentement du titulaire de l'autorité parentale est requis s'agissant du traitement de données concernant un mineur, cet âge devant se situer entre 13 et 16 ans (article 8) ;

– pour prévoir des exemptions, dérogations ou conditions spécifiques pour certaines catégories de traitement : traitements journalistiques, accès aux documents officiels, numéro d'identification national, données des salariés, traitement à des fins archivistiques, statistiques, de recherche scientifique (articles 85 à 89).

---

(1) Annexe 1.

Ainsi que l'ont souligné la plupart des personnes auditionnées par la mission, ces nombreux renvois aux droits nationaux font peser **le risque d'une nouvelle fragmentation** du régime de la protection des données personnelles dans l'Union européenne. Une telle situation aurait des effets négatifs sur l'effectivité de cette protection ainsi que sur la lisibilité de leurs obligations par les responsables de traitement et les sous-traitants. Elle créerait en outre un risque de mise en concurrence des systèmes juridiques par une recherche des tribunaux les plus favorables (« *forum shopping* » [(1)]) que le règlement visait justement à éviter.

B. LE RENFORCEMENT DES DROITS DES PERSONNES PHYSIQUES

1. L'évolution de la définition des données protégées

La notion de données à caractère personnel dans le règlement du 27 avril 2016

L'article 4, paragraphe 1, définit les données à caractère personnel comme : « *toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Le règlement reprend ainsi le socle de la définition des données personnelles par la directive de 1995 et le complète par des éléments nouveaux, adaptés à l'évolution du numérique. Le considérant 30 précise que les « *identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence* [...] *peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier* [l]*es personnes.* »

Ainsi que le précise le considérant 27 du règlement, celui-ci ne s'applique en revanche pas aux données à caractère personnel des personnes décédées, dont les règles de traitement relèvent des États membres.

La définition des **données sensibles**, dont le traitement est en principe interdit, a également été complétée par rapport à la directive de 1995 : les données biométriques et génétiques, ainsi que les données relatives à l'orientation sexuelle, ont été ajoutées à la liste en vigueur (article 9 du règlement).

(1) Le forum shopping *est un terme informel anglais de droit international privé, qui désigne la possibilité qu'offre à un demandeur la diversité des règles de compétences internationales de saisir les tribunaux des pays appelés à rendre la décision la plus favorable à ses intérêts.*

2. Le renforcement du consentement

Le règlement ne modifie pas les différentes conditions de licéité du traitement définies par la directive de 1995 (1), au premier rang desquelles figure le consentement de la personne concernée.

En revanche, il renforce les conditions applicables à ce consentement. La seule exigence posée par la directive de 1995 était en effet que le consentement devait avoir été donné « *indubitablement* » par la personne concernée. L'imprécision de cette notion ne paraissait plus adaptée au monde numérique, ainsi que l'a souligné la commission de réflexion sur les droits et libertés à l'ère du numérique : « *le consentement peut se heurter, dans l'environnement numérique actuel, à plusieurs limites* [...] *: complexification et sophistication des dispositifs techniques et des modèles commerciaux de collecte des données, sous-estimation par les individus des risques et des dommages potentiels générés par ces traitements de données, opacité ou surformalisation des informations délivrées par les responsables de traitement (recours à des politiques de vie privée ou* privacy policies *longues et complexes), interrogations sur le recueil d'un consentement véritablement libre par ces derniers.* » (2)

Le règlement précise la définition de l'expression du consentement, en posant le principe du **consentement explicite**. L'article 4 dispose en effet que le consentement correspond à *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*.

Le considérant 32 précise que le consentement peut être donné « *en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement que la personne concernée accepte le traitement* [...] ». Le consentement est exclu en cas de silence ou de cases précochées. Lorsqu'il s'agit d'une demande de consentement par voie électronique, celle-ci ne doit pas perturber l'utilisation du service qu'elle concerne.

Le consentement doit porter sur « *une ou plusieurs finalités spécifiques* » (article 6).

L'article 7 précise les conditions applicables au consentement :

– si celui-ci est donné dans une déclaration écrite concernant également d'autres questions (par exemple des conditions générales), « *la demande de*

---

(1) Cf. supra.

(2) Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, co-présidée par M. Christian Paul et Mme Christiane Féral-Schuhl, n° 3119, 9 octobre 2015.

consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples » ;

– le responsable de traitement doit être en mesure de prouver que la personne a consenti au traitement de ses données ;

– la personne concernée a le droit de retirer son consentement à tout moment mais ce retrait n'a pas d'effet rétroactif.

La personne concernée doit disposer d'une véritable liberté de choix et doit pouvoir refuser ou retirer son consentement sans subir de préjudice. Le consentement est présumé ne pas avoir été donné librement si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à cette exécution. (1)

En outre, le règlement définit **les conditions spécifiques applicables au consentement des enfants**, ce qui est une nouveauté par rapport à la directive 95/46. Le considérant 38 justifie cette protection spécifique par le fait que les enfants peuvent être moins conscients des risques, des conséquences, des garanties et de leurs droits en matière de traitement de données personnelles. Sont citées notamment l'utilisation des données personnelles d'un enfant à des fins de marketing, de création de profils de personnalité ou d'utilisateur et la collecte de données lors de l'utilisation de services proposés directement à un enfant.

L'article 8 définit le régime du consentement des enfants *: «* […] *en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. »* Le responsable du traitement doit *« s'efforcer de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles »*. Le recueil effectif du consentement auprès du titulaire de l'autorité parentale ne semble à cet égard pas totalement garanti.

Les États membres peuvent prévoir par la loi un âge inférieur à partir duquel l'enfant peut donner personnellement son consentement, cet âge ne pouvant être inférieur à 13 ans. À défaut de dispositions nationales spécifiques, l'âge de 16 ans s'appliquera.

(1) Considérants 42 et 43 ; article 7, paragraphe 4.

3. L'extension du droit à l'information

La directive 95/46 prévoyait déjà que les responsables de traitement devaient transmettre aux personnes concernées un certain nombre d'informations. Le champ de ces informations est élargi par les articles 13 et 14 du règlement.

Outre les informations déjà requises actuellement, les informations suivantes devront être fournies :

– les intérêts légitimes fondant éventuellement le traitement ;

– l'intention du responsable de traitement d'effectuer un transfert des données vers un pays tiers ;

– la durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

– le droit de demander l'effacement des données ou une limitation du traitement ;

– l'existence d'une prise de décision automatisée, y compris le profilage ;

– l'intention du responsable de traitement d'effectuer un traitement ultérieur pour une finalité autre.

Lorsque les données n'ont pas été collectées auprès des personnes concernées, le responsable de traitement devra indiquer, en outre, les catégories de données concernées et leur source.

En application de l'article 12, les informations doivent être transmises « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant* ». Elles peuvent être accompagnées d'icônes normalisées.

De manière plus générale, **l'article 5 (a) fait de la transparence l'un des principes du traitement des données personnelles**, explicité dans le considérant 39, qui précise que les personnes concernées par un traitement devraient également être informées « *des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement* ».

4. L'affirmation de nouveaux droits

a. Le droit à l'effacement (« droit à l'oubli »)

Dans ses réponses au questionnaire écrit des rapporteurs, la direction des affaires civiles et du Sceau (DACS) du ministère de la justice indique que « *le « droit à l'oubli » recoupe différents droits que sont, d'une part, le droit au*

déréférencement (effacement d'un lien) consacré par l'arrêt de la CJUE du 13 mai 2014 Google Spain et, d'autre part, le droit à l'effacement de la donnée à caractère personnel que l'article 17 du règlement (UE) 2016/679 instaure. »

Cet article définit le droit à l'effacement comme « *le droit* [pour une personne] *d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractères personnel la concernant* ».

Les responsables de traitement auront l'obligation d'effacer les données personnelles dans les cas suivants :

– elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

– la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;

– la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement à des fins de prospection ;

– les données à caractère personnel ont fait l'objet d'un traitement illicite ;

– les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

– les données à caractère personnel ont été collectées auprès d'enfants.

Sans être reconnu comme tel, le droit à l'effacement avait déjà une existence par le biais des dispositions de la directive 95/46 et de la loi du 6 janvier 1978 imposant que la durée de conservation des données n'excède pas celle nécessaire aux finalités de la collecte et du traitement [(1)].

Outre l'élargissement des motifs ouvrant droit à l'effacement des données, en particulier lorsque les données ont été collectées auprès d'enfants, le règlement innove en prévoyant que les responsables de traitement qui avaient rendu les données publiques et qui auront été tenus de les effacer devront prendre « *des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données* [...]*, ou de toute copie ou reproduction de celles-ci* ». Il s'agit cependant **uniquement d'une obligation de moyens** qui ne garantit pas l'effacement général des données et n'empêche pas leur éventuelle réutilisation publique ou privée.

(1) Article 6, paragraphe 1, de la directive 95/46 et article 6 (5°) de la loi du 6 janvier 1978.

Le paragraphe 3 de l'article 17 prévoit différentes limites : le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information ; pour respecter une obligation légale ou exécuter une mission d'intérêt public ; pour des motifs d'intérêt public dans le domaine de la santé publique ; à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques ; à la constatation, à l'exercice ou à la défense des droits en justice.

b. Le droit à la portabilité des données

L'article 20 du règlement prévoit un nouveau droit à la portabilité des données : les personnes concernées par un traitement auront « *le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* ». Ce droit peut s'exercer à condition que le traitement soit fondé sur le consentement ou sur l'exécution d'un contrat. Lorsque cela est possible techniquement, les données doivent pouvoir être transmises directement d'un responsable de traitement à un autre.

Par rapport au droit à la communication des données personnelles déjà prévu par la directive 95/46, **le droit à la portabilité impose la transmission des données dans un format réutilisable**.

La consécration du droit à la portabilité vise à assurer le renforcement du « *contrôle que les personnes concernées exercent sur leurs propres données* », comme l'énonce le considérant 68 du règlement, ce qui, dans un monde de plus en plus connecté, va renforcer la responsabilité individuelle, et impose donc un devoir d'éducation et d'information en direction de la population, à tous les âges.

Outre cet apport au regard des droits des personnes, le droit à la portabilité crée d'importantes opportunités économiques s'agissant du développement de nouveaux services et de nouvelles applications, par exemple en matière de consommation énergétique, ainsi que l'a souligné M. Henri Verdier, directeur interministériel des systèmes d'information et de communication, lors de son audition.

Le G29 a adopté en décembre 2016 des lignes directrices relatives à la portabilité, précisant l'étendue de ce droit et les obligations des responsables de traitement [(1)].

Ces lignes directrices clarifient notamment la notion de « données personnelles fournies par les personnes concernées » :

(1) G29, Guidelines on the right to data portability, 13 décembre 2016; 16/EN, WP242.

– ces données peuvent inclure des données concernant des tiers (par exemple des relevés téléphoniques comportant les appels entrants et sortants) ;

– il s'agit des données fournies activement et délibérément par les personnes concernées mais aussi des données générées et collectées à partir de leurs activités, par l'utilisation d'un service ou d'un dispositif (historique de recherche, données de trafic ou de localisation) ; en revanche ne sont pas concernées les données déduites ou dérivées des données fournies par les personnes, qui sont créées par le responsable de traitement.

Les lignes directrices précisent également que le droit à la portabilité ne devra pas porter atteinte aux droits et libertés des tiers, par exemple en les empêchant d'exercer leurs droits (droits d'accès, d'opposition). Les données des tiers ne pourront faire l'objet d'un traitement par le responsable auquel elles auront été transmises que si celui-ci est licite au sens du règlement, par exemple, s'il se fonde sur l'intérêt légitime du responsable de traitement qui fournit un service à la personne ayant transféré les données, dans le cadre d'une activité strictement personnelle ou domestique.

c. Le recours aux actions collectives

L'article 80, paragraphe 1, du règlement prévoit que les personnes concernées ont « *le droit de mandater un organisme, une organisation ou une association à but non lucratif, constituée conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant* » pour introduire en leur nom une réclamation auprès d'une autorité de contrôle ou un recours juridictionnel contre une autorité de contrôle ou contre un responsable de traitement ou un sous-traitant. Si le droit de l'État membre le prévoit, l'organisme ou l'association peut exercer le droit d'obtenir réparation au nom des personnes concernées.

En application du paragraphe 2 du même article, les États membres peuvent également autoriser les organismes ou associations à introduire des réclamations auprès de l'autorité de contrôle ou un recours juridictionnel, indépendamment de tout mandat des personnes concernées, s'ils estiment que les droits de ces personnes ont été violés du fait du traitement.

5. La question du profilage

La définition du profilage dans le règlement du 27 avril 2016

L'article 4 du règlement définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

Le profilage faisait déjà l'objet d'un encadrement par la directive 95/46 (article 15 relatif aux « *décisions individuelles automatisées* »).

L'article 22, paragraphe 1, dispose que « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire*. » Le considérant 71 cite comme exemples de telles décisions le rejet automatique d'une demande de crédit en ligne ou les pratiques de recrutement en ligne sans aucune intervention humaine.

Cette disposition ne s'appliquera pas si la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, si elle est autorisée par le droit de l'Union ou le droit de l'État membre ou si elle se fonde sur le consentement explicite de la personne concernée. Par rapport à la directive 95/46, **le règlement ajoute le consentement explicite comme fondement du profilage**.

Lorsque la décision pourra être fondée sur le profilage, le responsable de traitement devra mettre en place, en application de l'article 22, paragraphe 3, « *des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision*. » **L'encadrement du profilage est précisé** car la directive 95/46 ne faisait référence qu'à « *des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissant la sauvegarde de son intérêt légitime* » [(1)].

Le règlement prévoit par ailleurs une information spécifique : les personnes concernées devront être informées de l'existence du profilage et disposer d'informations sur la « *logique sous-jacente, ainsi que l'importance et les conséquences prévues* » du traitement (article 14, paragraphe 2). Les représentants de la Commission européenne rencontrés par vos rapporteurs leur ont précisé qu'il

(1) Article 15 de la directive 95/46.

ne s'agissait pas de la communication des algorithmes eux-mêmes, ceux-ci étant protégés en tant que secrets commerciaux.

Enfin, en application de l'article 35, paragraphe 3, une analyse d'impact devra être réalisée par le responsable de traitement lorsque des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire seront fondées sur le profilage.

C. LES PRINCIPES S'IMPOSANT AUX OPÉRATEURS TRAITANT DES DONNÉES PERSONNELLES

Le chapitre IV du règlement réunit, au sein des articles 24 à 43, l'ensemble des règles applicables aux responsables de traitement et aux sous-traitants c'est-à-dire les obligations générales qu'ils doivent respecter (section 1), les règles relatives à la sécurité des données à caractère personnel (section 2), celles relatives aux analyses d'impact (section 3) au délégué à la protection des données (section 4) et aux codes de conduite et à la certification (section 5).

L'ensemble de ces règles sont marquées par trois innovations majeures du règlement, saluées par l'ensemble des personnes entendues par la mission : la reconnaissance d'une responsabilité conjointe des responsables de traitement et des sous-traitants, l'extension du champ d'application de la réglementation européenne en matière de protection des données et le passage d'une logique de contrôle préalable des responsables de traitement à une logique de responsabilité.

1. Un périmètre étendu d'application

a. Responsable de traitements et sous-traitant : une responsabilité conjointe

Alors que la directive 95/46/CE concerne essentiellement les responsables de traitement [(1)], le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement. En effet, le considérant 18 précise que le règlement s'applique « *aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques* » [(2)].

Le règlement « égalise » les obligations applicables aux sous-traitants et aux responsables de traitements, qui verront leur responsabilité conjointement engagée en cas de manquement.

---

(1) Les responsables de traitement sont définis comme les organismes qui déterminent les finalités et les modalités de traitement de données personnelles.

(2) Le paragraphe 8 de l'article 4 du règlement reprend la définition du sous-traitant de la directive 95/46/CE, le sous-traitant étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitements ».

La question de la responsabilité conjointe des responsables de traitement et des sous-traitants a fait l'objet de débats nourris au Parlement européen, ce dernier étant favorable à l'affirmation d'une responsabilité solidaire, quels que soient le type de manquement et son origine. La France, à l'instar de certaines autres délégations, préférait une responsabilité conjointe, afin d'apporter une meilleure sécurité juridique aux entreprises quant aux conditions dans lesquelles leur responsabilité pouvait être engagée, compte tenu par ailleurs du niveau très élevé des sanctions encourues [(1)] . C'est cette option qui a été retenue.

Comme le prévoit actuellement la directive, le règlement précise que le responsable de traitements ne peut faire appel qu'à des sous-traitants présentant des garanties suffisantes permettant de répondre aux exigences du règlement. À ce titre, l'adhésion du sous-traitant à un code de bonne conduite (article 40 du règlement) ou à un mécanisme de certification approuvé (article 42 du règlement) constitue une forme de garantie.

Si le principe de contractualisation entre le responsable de traitements et le sous-traitant reste en vigueur, le contenu du contrat est, lui, enrichi. Ce dernier doit dorénavant préciser les obligations mises à la charge du sous-traitant qui peut désormais être tenu responsable de ses manquements au titre de la protection des données. Il définit notamment, en application du paragraphe 3 de l'article 28 du règlement « *l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement* ».

Par ailleurs, la possibilité laissée à un sous-traitant de sous-traiter tout ou partie de la prestation qui lui a été confiée doit faire l'objet d'un accord écrit préalable du responsable de traitement. Les obligations contractuelles que le responsable de traitement aura mises à la charge du sous-traitant de premier rang seront répercutées aux prestataires de second rang (article 28 paragraphe 2 du règlement).

Lors de son audition par la mission, M. Massimo Bucalossi, vice-président de la commission « intranet et nouvelles technologies » du Conseil national des barreaux, a salué la reconnaissance de la responsabilité des sous-traitants en faisant remarquer que ces derniers pouvaient en pratique traiter davantage de données personnelles que les responsables de traitement. C'est le cas par exemple des sociétés qui font du « mailing » [(2)] pour des associations.

---

(1) Dans le cas d'une responsabilité solidaire, un créancier peut se retourner contre n'importe lequel des associés d'une entreprise pour obtenir le règlement de l'ensemble des dettes, À l'inverse, dans une responsabilité conjointe, le créancier ne peut demander à un associé que le remboursement d'une dette à la hauteur de sa participation dans la société.

(2) Le « mailing *», qui est initialement le terme anglais pour désigner un publipostage courrier, est une campagne de marketing direct qui consiste à envoyer une proposition commerciale plus ou moins personnalisée par voie postale à un ensemble d'individus soigneusement ciblés.*

b. Une application extra-territoriale du règlement

Le règlement s'applique quelle que soit la forme juridique de l'établissement concerné. Son considérant 22 précise, en effet, que : « *L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard*. » (1)

Par ailleurs, le champ d'application territorial du règlement a été élargi pour le mettre en conformité avec la jurisprudence de la Cour de justice de l'Union européenne dans l'arrêt *Google c/Espagne* rendu le 13 mai 2014. Celle-ci a, en effet, considéré que la directive était territorialement applicable bien que le traitement soit effectué par Google Inc. – dont le siège social est établi à Mountain View – tandis que l'activité de Google Spain, établissement qui a son siège à Madrid, se limitait à la promotion des ventes d'espaces publicitaires. Même si le traitement n'était pas réalisé par l'établissement espagnol, la Cour de justice a relevé qu'il suffisait qu'il soit réalisé « dans le cadre » de ses activités pour se voir appliquer la directive (2).

Ainsi, le règlement s'applique aux entreprises qui ne sont pas établies sur le territoire de l'Union européenne mais qui traitent des données de personnes qui se trouvent sur le territoire de l'Union européenne. En effet, en application des considérants 23 et 24 du règlement, un responsable de traitements ou un sous-traitant qui ne dispose pas d'un établissement au sein de l'Union européenne se verra tout de même soumis au règlement :

– **lorsque ses activités de traitement sont liées à une offre de biens ou de services à des personnes qui se trouvent sur le territoire de l'Union européenne, qu'un paiement soit exigé ou non.**

Le règlement précise que des facteurs tels que « *l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union* » (3) peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes qui se trouvent sur le territoire de l'Union européenne. (4)

---

(1) Selon la Cour de justice, la présence d'un représentant, d'une adresse et d'un compte bancaire au sein d'un État membre suffit à caractériser cette activité (CJUE, 1er octobre 2015, aff. C-230/14, Weltimmo : JurisData n° 2015-025844).

(2) Cf. infra.

(3) Considérant 23 du règlement.

(4) En revanche, la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union européenne, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement ne suffisent pas pour établir l'intention d'offrir des biens ou des services à des personnes qui se trouvent dans l'Union européenne.

– **lorsque le traitement est lié au suivi du comportement des personnes qui se trouvent sur le territoire de l'Union européenne**.

Le règlement indique que sont concernées notamment les techniques de profilage d'une personne physique permettant « *notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* ». (1)

En pratique, le droit européen s'appliquera chaque fois qu'un résident européen, quelle que soit sa nationalité, sera directement visé par un traitement de données, y compris par internet et par le biais d'objets connectés (par exemple les montres connectées, les objets mesurant l'activité physique, les appareils domotiques, consoles de jeux connectées), quels que soient la nature et la localisation du support de stockage et de traitement (2).

Les responsables de traitement ou les sous-traitants devront désigner par écrit un représentant au sein de l'Union européenne pour assurer leur représentation juridique, même s'ils ne disposent pas d'un établissement (3). Cette désignation n'exonère en rien le responsable de traitements de sa responsabilité « *puisque la désignation d'un représentant est sans préjudice d'actions en justice qui pourraient être intentées contre les responsables du traitement et sous-traitant eux-mêmes* » (article 27 du règlement).

2. D'une logique de contrôle préalable à une logique de responsabilité

a. Une logique de conformité et de responsabilité

Comme le rappelle la CNIL dans les éléments transmis à la mission : *« Si le contrôle* a posteriori *a gardé sa pertinence, les déclarations ont perdu une large partie de leur raison d'être. La question que se posent les responsables de traitement a changé : il ne s'agit plus de savoir d'abord si la bonne " formalité " a été faite, mais de savoir si l'entité assure une protection optimale des données à chaque instant.* »

Ainsi, alors que la directive de 1995 reposait en grande partie sur l'existence de formalités préalables (déclaration, autorisations), le règlement européen, qui tient compte de ces évolutions fondamentales, repose sur une logique de conformité et de responsabilité, dite d'« *accountability* ».

Dans une étude consacrée au règlement dans la revue de droit bancaire et financier, les auteurs constatent : « L'accountability *est une notion difficilement*

(1) Considérant 24 du règlement.

(2) Ainsi que l'a précisé le G29 dans un avis du 16 septembre 2014, la directive 95/46 s'applique déjà à ce type de traitements (avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, 1471/14/FR,WP 223).

(3) A l'exception des autorités publiques de pays tiers, et des responsables de traitement mettant en œuvre des traitements de données occasionnels et qui ne présentent pas de risques. Ils restent toutefois soumis aux autres dispositions du règlement.

traduisible dans toutes ses nuances en français. Le terme " responsabilité " *lui est souvent substitué mais il n'évoque que l'une des facettes de la notion.* L'accountability *est, à la fois, l'affirmation de la responsabilité de l'entreprise mais aussi, et surtout, sa faculté à démontrer qu'elle a bien respecté les exigences réglementaires en matière de protection des données*. » (1)

La contrepartie de cette responsabilisation des acteurs est la suppression de la plupart des obligations déclaratives, **dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes**. (2)

L'article 30 du règlement remplace ainsi la notification générale de traitement des données à l'autorité de contrôle, exigée par la directive n° 95/46/CE par l'obligation, pour les responsables de traitement et les sous-traitants, de garder un registre des activités de traitement de données effectuées sous leur responsabilité.

b. Les nouvelles obligations pesant sur les entreprises

Les nouveaux outils de mise en conformité des responsables de traitement et des sous-traitants sont la mise en place de mesures de protection des données appropriées, la tenue d'un registre des activités de traitement de données, la mise en place d'études de l'impact des traitements sur la vie privée et d'un délégué à la protection des données (DPO), la notification de failles de sécurité aux autorités et aux personnes concernées et des démarches de certification ou de code de bonne conduite.

- *La protection des données dès la conception et la protection des données par défaut*

La responsabilisation des entreprises s'incarne par les **principes de la « protection des données dès la conception »** (*privacy by design*) et de **« protection des données par défaut »** (*privacy by default*). Ces principes imposent aux responsables du traitement des données de mettre en œuvre toutes les techniques nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

---

(1) « Le règlement sur la protection des données : les 10 commandements à connaître pour passer de la théorie à la pratique », par M. Emmanuel Jouffin, responsable juridique de banque, M. Xavier Lemarteleur, responsable juridique Technologies de l'information et Mme Marie-Noëlle Gibon, correspondante informatique et liberté du groupe La Poste et La Banque Postale, Revue de Droit bancaire et financier (n° 4, Juillet 2016, étude 18).

(2) Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

La définition du « *privacy by design* » et du « *privacy by default* » dans le règlement

L'article 25 du règlement affirme ainsi que le responsable de traitement « *met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.* »

Celui-ci met en œuvre les mesures techniques et organisationnelles appropriées « *pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée*. »

Concrètement, ces deux principes impliquent que les données traitées soient limitées à ce qui est strictement nécessaire à la finalité du traitement, que des durées de conservation aient été fixées, qu'il existe des règles de suppression automatique des données et qu'un processus d'habilitation soit mis en place pour l'accès aux données personnelles au bénéfice des seules personnes ayant à en connaître.

Parmi les techniques de sécurisation, le règlement évoque le chiffrement [(1)] et la pseudonymisation des données [(2)].

- *L'obligation de tenir un registre des activités de traitement de données*

Afin de démontrer qu'ils ont mis en place des mesures de protection des données appropriées, l'article 30 du règlement prévoit que les responsables de traitement et les sous-traitants ont l'obligation de tenir un **«** *registre des activités de traitement effectuées sous leur responsabilité* », ce registre étant mis à la disposition de l'autorité de contrôle à sa demande.

Le paragraphe 5 de l'article 30 précise cependant que cette obligation ne s'applique pas à une entreprise ou à une organisation **comptant moins de 250 employés**, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de

(1) Selon la CNIL : « le chiffrement d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. (…) Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines. » https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

(2) Cf. supra.

données visées au paragraphe 1 de l'article 9 [1], ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 [2] .

Ce registre, qui se présente sous forme écrite, devra être tenu à la disposition de l'autorité de contrôle et permettra à cette dernière de vérifier que l'entreprise a bien pris en compte la protection des données et que celle-ci est respectueuse de la réglementation en la matière.

Le registre des activités de traitement

En application du paragraphe 1 de l'article 30 du règlement, le responsable de traitements doit tenir un registre comportant les informations suivantes :

– le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

– les finalités du traitement ;

– une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

– les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

– les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49 du règlement, les documents attestant de l'existence de garanties appropriées ;

Dans la mesure du possible, doivent aussi figurer les délais d'effacement des données et les mesures de sécurité mises en place.

Le paragraphe 2 de l'article 30 précise les informations contenues dans le registre tenu par le sous-traitant.

Concrètement les entreprises qui ont nommé un correspondant « informatique et liberté », comme leur en laissait la possibilité la loi du 6 janvier 1978 [3] et le décret du 20 octobre 2005 [1], disposent déjà d'un registre interne que ce correspondant est chargé de tenir. Il devra néanmoins être complété.

---

(1) L'article 9 du règlement dispose que « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. *»*

(2) L'article 10 du règlement prévoit que « Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un 'État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. *»*

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

- *L'obligation de faire une analyse de l'impact des opérations de traitement sur la protection des données à caractère personnel*

L'article 35 du règlement prévoit que des **analyses de l'impact des opérations de traitement sur la protection des données à caractère personnel** devront être conduites par les responsables de traitement « *lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ».

Ainsi, pour tous les traitements à risque et préalablement à ceux-ci, le responsable devra conduire une étude d'impact faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées.

L'article 35 précise qu'une analyse d'impact est obligatoire :

– lorsque le traitement consiste en une « *évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire* » ;

– lorsque sont traitées à grande échelle des catégories particulières de données visées au paragraphe 1 de l'article 9 du règlement [(2)] ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du règlement [(1)] ;

– lorsque le traitement consiste en une surveillance systématique à grande échelle d'une zone accessible au public.

La CNIL a précisé, quant à elle, qu'étaient concernés les traitements de données sensibles [(3)], et les traitements reposant sur « *l'évaluation systématique et approfondie d'aspects personnels des personnes physiques* », c'est-à-dire notamment sur des techniques de profilage [(4)].

En cas de risque élevé, le responsable de traitements doit consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Cette dernière pourra s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

---

(1) Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Cf. supra.

(3) Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques.

(4) https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

Plusieurs personnes entendues par la mission ont considéré que la notion de « risque élevé » restait floue. Afin de la préciser, l'article 35 du règlement prévoit que les autorités de contrôle :

– établiront et publieront une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise ;

– pourront aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

L'article 35 du règlement précise que ces listes sont transmises au comité européen de protection des données afin de garantir que des critères compatibles sont adoptés au sein de l'Union européenne.

En outre, le G29 mène actuellement des travaux sur cette question et devrait adopter des lignes directrices au premier trimestre 2017. Cet avis devrait clarifier notamment :

– la notion de traitement pouvant engendrer des risques élevés pour lesquels une analyse d'impact relative à la protection des données est obligatoire ;

– les critères permettant de déterminer qu'une méthodologie d'analyse d'impact est compatible avec les exigences du règlement ;

– les conditions de consultation préalable de l'autorité, en application de l'article 36 du règlement.

- *L'obligation de désigner un délégué à la protection des données*

L'article 37 du règlement prévoit la mise en place d'un délégué à la protection des données par certains responsables de traitement et sous-traitants.

La désignation d'un délégué à la protection des données sera obligatoire lorsque le traitement est effectué par une autorité publique ou un organisme public « *à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle* ».

S'agissant des organismes privés, cette désignation sera obligatoire lorsque :

– les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui « *du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées* » ;

– les activités de base du responsable du traitement ou du sous-traitant consistent en « *un traitement à grande échelle de catégories particulières de*

données visées à l'article 9 [du règlement] [(1)] *et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10* [du même règlement] [(2)] ».

Les organismes publics devant désigner un délégué à la protection des données

Le G29, dans des lignes directrices relatives au délégué à la protection personnelle (DPO) publiées le 13 décembre 2016 [(2)], rappelle que le règlement ne définit pas ce qu'est une « autorité ou un organisme public ». Si cette notion doit être déterminée en application du droit national, le G29 précise néanmoins que seront concernés les autorités nationales, régionales et locales, mais aussi les organismes de droit public et des personnes physiques ou morales de droit public ou privé, dans des secteurs tels que les services de transport public, de l'approvisionnement en eau et en énergie, des infrastructures routières, de la radiodiffusion de service public, du logement public ou des instances disciplinaires pour les professions réglementées. Dans ces cas, la désignation d'un DPO est obligatoire.

Bien qu'il n'y ait aucune obligation dans de tels cas, le G29 recommande qu'un délégué à la protection des données soit désigné dans des organismes privés exerçant des fonctions publiques ou exerçant une autorité publique et que l'activité de ce DPO concerne toutes les opérations de traitement effectuées, y compris celles qui ne sont pas liées à l'exécution d'une tâche publique (par exemple, la gestion d'une base de données).

L'article 37 du règlement précise que le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, « *de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions* ».

Le délégué à la protection des données personnelles peut être un membre du personnel du responsable de traitement ou du sous-traitant, il peut aussi être externe à l'entreprise et accomplir ses missions dans le cadre d'un contrat de service. Il n'est pas nécessairement exclusivement dédié à la protection des données, il peut ainsi avoir d'autres missions, à charge, pour le responsable de traitement, de veiller à ce que ces missions n'entraînent pas de conflits d'intérêts.

Le responsable du traitement et le sous-traitant doivent veiller à ce que le délégué à la protection des données :

– soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;

– dispose de toutes les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement ;

---

(1) *Cf.* supra.

(2) https://www.cnil.fr/sites/default/files/atoms/files/dpoen.pdf

– ne reçoive aucune instruction en ce qui concerne l'exercice des missions (il ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions) ;

Ce délégué est chargé :

– d'informer et de conseiller le responsable de traitements ou le sous-traitant, ainsi que ses employés ;

– de contrôler le respect du règlement européen et du droit national en matière de protection des données ;

– de conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ;

– de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Concrètement les entreprises qui ont nommé un correspondant « informatique et liberté » (CIL), comme leur en laissaient la possibilité la loi du 6 janvier 1978 et le décret du 20 octobre 2005, ont déjà une personne en leur sein dont les fonctions sont dédiées la protection des données. 18 000 organismes sont aujourd'hui dotés d'un tel correspondant. En revanche, comme le montre le tableau ci-dessous, ces entreprises devront procéder à certains aménagements, les fonctions du DPO étant plus larges que celles du CIL. Par ailleurs, la liste des traitements actuellement tenus par les CIL ne coïncide pas avec le registre de des activités de traitement.

LE STATUT ET LES MISSIONS DU CIL ET DU DPO

		CIL	**DPO**
Statut	Caractère obligatoire	Non	Oui
	Indépendance fonctionnelle	Oui	Oui
	Rattachement au plus haut niveau de la direction du responsable de traitement	Non	Oui
	Obligation du responsable de traitements de fournir les moyens	Oui	Oui
	Expertise attestée	Non	Oui
	Externalisation	Condition de seuil	Sans condition
	Secret professionnel	Non	Oui
	À l'abri des conflits d'intérêts	Oui	Oui
Missions	Assurer le respect de la législation	Veille	Oui
	Contrôle a priori formalisé pour les traitements à risques	Facultatif	Oui
	Sensibilisation	Oui	Oui
	Supervision des audits	Non	Oui
	Saisine directe par les personnes concernées	Non	Oui
	Avis sur les études d'impact sur la vie privée	Non prévu	Oui

	Correspondant de la CNIL	Oui	Oui
	Droit d'alerte	Oui	Non prévu
	Coopération avec la CNIL	Non	Oui

Source : « Le règlement sur la protection des données : les 10 commandements à connaître pour passer de la théorie à la pratique », *par M. Emmanuel Jouffin, responsable juridique de banque, M. Xavier Lemarteleur, responsable juridique Technologies de l'information et Mme Marie-Noëlle Gibon, correspondante informatique et liberté du groupe La Poste et La Banque Postale, Revue de Droit bancaire et financier (n° 4, juillet 2016, étude 18).*

- *L'obligation de notification des violations de données à caractère personnel*

Lorsqu'il constate une violation de données à caractère personnel, le responsable du traitement des données doit la **notifier à l'autorité nationale de protection des données dans un délai de 72 heures**, « *à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* » (article 33 du règlement) (1)

Par ailleurs l'article 34 prévoit que l**'information des personnes concernées** est requise si cette violation est susceptible d'engendrer « un risque élevé » pour les droits et libertés de ces personnes.

La notification de la violation des données personnelles à la personne concernée

La communication auprès de la personne concernée doit intervenir dans les meilleurs délais et dans des termes « *clairs et simples* ». Les informations communiquées visent, la nature de la violation, les coordonnés du délégué à la protection des données, les conséquences probables de la violation, une description des mesures prises ou à prendre pour remédier à la violation. L'autorité de contrôle a la faculté d'exiger du responsable du traitement qu'il procède à cette communication (art. 34 du règlement).

Une telle information individuelle n'est pas nécessaire si l'une des conditions suivantes est remplie :

– les mesures de protection techniques et organisationnelles appropriées notamment le chiffrement des données ont été prises ;

– des mesures ultérieures garantissant que le risque pour les droits et libertés des personnes n'est plus susceptible de se matérialiser ont été prises ;

– si la communication individuelle exige « *des efforts disproportionnés* », une communication publique ou une autre mesure étant alors possible.

Si le règlement ne définit pas ce qu'est une « *violation de données à caractère personnel* », l'article 34 bis I de la loi de 1978 la définit comme « *toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* ».

(1) Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

- *Développer les codes de bonne conduite et la certification pour favoriser le respect du règlement*

Le règlement réserve une place importante à des mécanismes tels que les codes de bonne conduite et la certification.

Ainsi la certification d'un responsable de traitement, ou d'un sous-traitant situé à l'étranger, pourra servir de base à un transfert de données vers l'étranger. De même, l'application d'un code de conduite ou l'obtention d'une certification pourra être utilisée pour démontrer le bon respect par le responsable de traitement ou un sous-traitant de ses obligations en matière de protection de données (article 25 du règlement), de garanties apportées par un sous-traitant (article 28 du règlement) ou de l'obligation de sécurités des données (article 32 du règlement). Enfin, lorsque l'autorité de contrôle envisage d'infliger une sanction administrative à une entreprise, le fait que cette dernière ait appliqué des codes de conduite, ou obtenu une certification, constitue un élément pris en considération afin de moduler ladite sanction (article 83 du règlement).

Les codes de bonne conduite et la certification dans le règlement

L'article 40 du règlement indique que les **codes de bonne conduite**, qui peuvent être élaborés par des associations ou des syndicats professionnels, peuvent être soumis et approuvés par l'autorité de contrôle. L'article 41 du règlement précise que le contrôle du respect du code de conduite peut être effectué « *par un organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'autorité de contrôle compétente* ».

Une **certification** est une démarche volontaire par laquelle l'entreprise fait constater la conformité de ses procédures en matière de protection des données à une norme avalisée par l'autorité de contrôle. Contrairement aux codes de conduites, la certification ne peut être délivrée que par un organisme de certification, celui-ci ayant été au préalable agréé par l'autorité de contrôle.

Dans les éléments transmis à la mission, la CNIL rappelle qu'elle dispose par rapport à ses homologues européens d'une expérience acquise en la matière, puisqu'elle délivre des labels depuis 2012. Cette mission est donc confortée et élargie par le règlement européen, puisque la CNIL pourra :

– délivrer des labels nationaux, sur la base de ses propres référentiels (4 à ce jour) et européens, sur la base de référentiels européens, approuvés par le comité européen de protection des données ;

– agréer des tiers certificateurs sur la base de critères approuvés par le comité européen de protection des données et sur la base de critères définis par elle ;

– contrôler la certification et les labels délivrés.

Des lignes directrices du G29 sont en cours d'élaboration sur ce sujet.

3. La sanction du non-respect des obligations

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de contrôle peuvent notamment prononcer un avertissement, mettre en demeure l'entreprise, limiter temporairement ou définitivement un traitement, suspendre les flux de données, ordonner de satisfaire aux demandes d'exercice des droits des personnes ou ordonner la rectification, la limitation ou l'effacement des données. S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

Mais surtout, l'article 83 du règlement donne aux autorités de contrôle la possibilité de prononcer des amendes administratives en complément ou à la place des mesures correctives. Celles-ci peuvent atteindre, selon la catégorie de l'infraction, **10 à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 % à 4 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

Peuvent faire l'objet d'amendes administratives pouvant s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, la violation des règles détaillées dans le tableau suivant :

DISPOSITIONS DU RÈGLEMENT DONT LA VIOLATION ENTRAÎNERA UNE AMENDE POUVANT S'ÉLEVER JUSQU'À 10 MILLIONS D'EUROS OU 2 % DU CHIFFRE D'AFFAIRES (1)

Obligations incombant au responsable du traitement et au sous-traitant
Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information (article 11)
Protection des données dès la conception et protection des données par défaut (article 25)
Responsables conjoints du traitement (article 26)
Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union (article 27)
Sous-traitant (article 28)
Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant (article 29)
Registre des activités de traitement (article 30)
Coopération avec l'autorité de contrôle (article 31)
Sécurité du traitement (article 32)
Notification à l'autorité de contrôle d'une violation de données à caractère personnel (article 33)
Communication à la personne concernée d'une violation de données à caractère personnel (article 34)
Analyse d'impact relative à la protection des données (article 35)

(1) Paragraphe 4 de l'article 83 du règlement.

Consultation préalable (article 36)
Désignation du délégué à la protection des données (article 37)
Fonction du délégué à la protection des données (article 38)
Missions du délégué à la protection des données (article 39)
Certification (article 42)
Organismes de certification (article 43)
Obligations incombant à l'organisme de certification
Certification (article 42)
Organismes de certification (article 43)
Obligations incombant à l'organisme chargé du suivi des codes de conduite
Prise de des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant (article 41)

La violation des règles fondamentales relatives au traitement des données ou aux droits des personnes concernées entraîne des amendes administratives d'un montant plus élevé pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent :

DISPOSITIONS DU RÈGLEMENT DONT LA VIOLATION ENTRAÎNERA UNE AMENDE POUVANT S'ÉLEVER JUSQU'À 20 MILLIONS D'EUROS OU 4 % DU CHIFFRE D'AFFAIRES

Principes de base d'un traitement, y compris les conditions applicables au consentement en application des articles 5 (principes relatifs au traitement des données à caractère personnel), 6 (licéité du traitement), 7 (conditions applicables au consentement) et 9 (traitement portant sur des catégories particulières de données à caractère personnel) du règlement.
Droits dont bénéficient les personnes concernées en application des articles 12 à 22 du règlement (traitement portant sur des catégories particulières de données à caractère personnel, informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée, informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, droit d'accès de la personne concernée, droit de rectification, droit à l'effacement, droit à la limitation du traitement, obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement, droit à la portabilité des données, droit d'opposition, décision individuelle automatisée, y compris le profilage)
Règles relatives aux transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale détaillées aux articles 44 à 49 ;
Obligations découlant du droit des États membres adoptées en application du chapitre IX du règlement
Non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58 du règlement

Ces montants doivent être rapportés au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement sur l'ensemble du territoire de toute l'Union européenne. Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

4. Une attention particulière doit être accordée aux TPE et aux PME

Pour tenir compte de la situation particulière des petites et moyennes entreprises, le règlement ne comporte qu'une dérogation qui concerne les entreprises occupant moins de 250 employés qui sont dispensées de la tenue de registre de traitement. Le considérant 13 renvoie la prise en compte de la situation PME aux législations nationales : « *les institutions et organes de l'Union, et les États membres et leurs autorités de contrôle sont en outre encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du (…) règlement*. »

Cependant, vos rapporteurs considèrent qu'une attention particulière devra être accordée aux petites et moyennes entreprises qui pourront, malgré cette dérogation, rencontrer des difficultés pour respecter les nouvelles obligations posées par le règlement. Beaucoup d'entreprises n'auront pas conscience de la portée de ces nouvelles obligations. La CNIL devra faire œuvre de pédagogie sur ce sujet. À ce titre, il pourrait être utile que des actions d'informations soient menées dans les chambres de commerce et d'industrie et les chambres de métiers et de l'artisanat.

M. Éric Barbry, président de la commission juridique de l'Association pour le commerce et les services en ligne (ACSEL) a rappelé que le règlement comprenait de nombreuses obligations nouvelles pour les entreprises, sans que des paliers soient prévus pour une mise en œuvre progressive et qu'il serait peu probable que toutes les entreprises soient prêtes en 2018. Il a notamment regretté que le règlement ne permette la mise en œuvre d'expérimentation, afin de permettre à de nouvelles *start-up* de tester de nouveaux développements de numériques sans être contraintes de respecter immédiatement l'ensemble des obligations du règlement.

De même, Mme Marie-Blanche Niel-Gilly, directrice des données personnelles et correspondante « informatique et libertés » de l'entreprise *SoLocal Group* a indiqué à la mission que la notification de failles de sécurité aux autorités de contrôle dans un délai de 72 heures pourrait être particulièrement contraignante pour les petites entreprises, qui ne seront pas en mesure de détecter des failles dans ce délai ou de gérer ce type de « crise ».

M. Marc Mossé, directeur juridique et affaires publiques Europe de *Microsoft* a quant à lui souligné le rôle essentiel que *Microsoft* devrait jouer en matière d'accompagnement des PME partenaires de l'entreprise pour leur expliquer les nouvelles obligations auxquelles elles seront soumises. Mme Marie-Charlotte Roques-Bonnet, directrice de la politique de confidentialité de cette même entreprise, a appelé l'attention de la mission sur le fait que la documentation que devraient réunir les responsables de traitement pour prouver la conformité de leur traitement aux exigences du règlement risquait de constituer des obligations très « bureaucratiques » pour des petites entreprises.

D. L'ENCADREMENT DES TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS

1. L'encadrement par le règlement des transferts de données à caractère personnel vers des pays tiers ou des organisations internationales

Si le règlement autorise les responsables de traitement et sous-traitants à transférer des données hors de l'Union européenne, ce n'est que dans la mesure où ces transferts garantissent un niveau de protection suffisant et approprié des données personnelles. Les données transférées hors Union restent soumises au droit de l'Union européenne non seulement pour leur transfert mais aussi pour tout traitement et transfert ultérieur.

Ces règles sont énoncées au chapitre V du règlement (« *Transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales* », articles 44 à 50).

L'article 44 précise le **principe général applicable aux transferts** : « *Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.* ».

L'article 45 autorise les transferts de donnée fondés sur une décision de la Commission constatant que le pays tiers assure un niveau de protection adéquat (« *transferts fondés sur une décision d'adéquation* »). Un tel transfert ne nécessite pas d'autorisation spécifique. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale [(1)].

(1) Le Royaume-Uni devra appliquer le règlement à partir du 25 mai 2018 mais ne sera plus lié par celui-ci après sa sortie de l'Union européenne. Pour permettre la circulation des données personnelles, il devra solliciter une décision d'adéquation auprès de la Commission.

Transferts de données : les critères de la décision d'adéquation de la Commission

Le paragraphe 2 de l'article 45 du règlement liste les éléments que doit prendre en compte la Commission afin de rendre sa décision d'adéquation, tels que l'État de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, l'existence d'autorités de contrôles indépendantes…

La Commission doit s'assurer que les éventuelles évolutions intervenues dans l'État tiers conservent intactes les garanties en matière de protection des données à caractère personnel pour les résidents européens.

Le règlement précise en particulier que le pays tiers devra assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres ; les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel.

En l'absence de décision d'adéquation de la Commission, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives (« *transfert moyennant des garanties appropriées* ». Ces garanties sont les suivants :

– un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;

– des règles d'entreprises contraignantes (« *transfert moyennant des garanties appropriées* ») détaillée au sein de l'article 47 du règlement ;

– des clauses types de protection des données adoptées par la Commission (article 46) ;

– des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission ;

– un code de conduite ou un mécanisme de certification assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées.

L'article 48 du règlement précise que toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être « *reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre* ».

Si aucune des conditions qui caractérisent ces types de transferts n'est remplie, l'article 49 permet un transfert dérogatoire pour des situations particulières qui sont énoncées de manière limitative aux points a) à g) du paragraphe 1 et au deuxième alinéa du même paragraphe. Il s'agit, par exemple, du transfert qui est « *nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement* ».

En tout état de cause, l'article 49 rappelle que lorsqu'un transfert vers un pays tiers ou une organisation internationale ne peut être réalisé dans les conditions détaillées aux articles 46 à 48, il peut avoir lieu que s'il « *ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.* » Dans ce cas, le responsable du traitement informe l'autorité de contrôle du transfert.

2. L'impact du règlement sur le « bouclier vie privée Union européenne-États-Unis »

L'entrée en vigueur du règlement pose la question de son articulation avec l'accord que la Commission a conclu en février 2016 avec les États-Unis sur le cadre des transferts transatlantiques de données.

En effet, comme il a été évoqué précédemment [(1)], la Cour de justice a invalidé la décision n° 2000/520/CE de la Commission, qui aurait permis l'entrée en vigueur de l'accord sur la Sphère de Sécurité, qui rendait possible le transfert de données personnelles entre l'Union européenne vers des entreprises américaines, au motif que ce pays ne présentait pas des garanties suffisantes en matière de protection des données personnelles [(2)]. À la suite de cet arrêt, la Commission a conclu en février 2016 un nouvel accord avec les États-Unis sur le cadre des transferts transatlantiques de données, le « bouclier vie privée Union européenne-États-Unis » (EU-US *Privacy shield*).

Adopté par la Commission le 12 juillet 2016 [(3)] et entré en vigueur le 1er août 2016, ce nouvel accord vise à tenir compte des exigences énoncées par la Cour de justice. Il impose aux entreprises des obligations renforcées en termes de traitement des données et d'information des personnes concernées par les traitements de données (article 1er). Il crée une supervision plus étroite. Les personnes concernées disposent de mécanismes de recours plus étendus en cas de

---

(1) Cf. supra.

(2) CJUE, 6 octobre 2015, C-362/14, Schrems.

(3) Décision d'exécution 2016/1250 (UE).

non-respect des principes du bouclier vie privée Union européenne-États-Unis. Il est prévu que le dispositif fasse l'objet d'une réévaluation annuelle pour s'assurer qu'il reste suffisamment protecteur des données transmises (article 4 de l'accord). Enfin, les entreprises destinataires des données doivent préalablement être inscrites sur un registre tenu par l'administration américaine.

La décision d'exécution de la Commission européenne intègre par anticipation, certaines des avancées prévues par le règlement, notamment concernant le rôle et les pouvoirs des autorités de contrôle, et introduit un mécanisme de vérification périodique. Cela répond à une demande forte de la France et de l'Allemagne, qui avaient appelé à une renégociation de l'accord sur la Sphère de Sécurité bien avant l'invalidation de celle-ci, afin de la mettre au niveau des exigences renforcées du règlement.

Le considérant 15 de la décision d'exécution de la Commission du 12 juillet 2016 précise que « *le bouclier de protection des données ne porte pas atteinte à l'application de la législation de l'Union régissant le traitement des données à caractère personnel dans les États membres* », la note de bas de page se référant explicitement au règlement européen.

À compter de l'entrée en application du règlement, cette décision suivra le régime général des décisions d'adéquation prévu par l'article 45 : elle sera notamment soumise à une révision périodique pour évaluer si le niveau de protection des données reste substantiellement équivalent à celui assuré par le droit de l'Union européenne. En pratique, la décision prévoit elle-même une procédure de révision périodique plus fréquente, puisqu'une revue conjointe doit être conduite tous les ans, en y associant les autorités de protection des données.

La pérennité du bouclier vie privée et sa conformité au règlement pourraient néanmoins être remises en cause dans les mois qui viennent.

En premier lieu, dans une déclaration du 29 juillet 2016, le G 29 a émis des réserves sur cet accord et a considéré que d'importantes préoccupations demeuraient concernant notamment l'accès par les autorités publiques américaines aux données transférées par l'Union européenne. Le G 29 ne se considère pas lié par la position de la Commission sur le niveau suffisant de protection garanti par l'accord et indique que la première évaluation annuelle conjointe de cet accord sera « un moment clé » permettant d'évaluer l'effectivité des garanties prévues par le bouclier vie privée.

Déclaration du G29 du 29 juillet 2016 relative à la décision de la Commission européenne concernant le *Privacy Shield*

Dans cette déclaration, le G29 rappelle que dans un avis du 13 avril 2016, il avait exprimé des inquiétudes et demandé diverses clarifications. Certaines d'entre elles ont été prises en compte par la Commission et les autorités américaines dans la version finale des documents relatifs au bouclier vie privée. Néanmoins, le G 29 considère que d'importantes préoccupations demeurent :

– en ce qui concerne le volet commercial, le G29 regrette, par exemple, le défaut de règles spécifiques pour les décisions automatisées et l'absence d'un droit d'opposition. La manière dont les principes du bouclier vie privée vont être appliqués aux sous-traitants mériterait d'être davantage explicitée ;

– en ce qui concerne l'accès par les autorités publiques aux données transférées aux États-Unis dans le cadre du bouclier vie privée, le G29 aurait souhaité des garanties plus strictes concernant l'indépendance du médiateur américain (Ombudsperson) et les pouvoirs qui lui sont accordés. Le G29 note l'engagement des services de renseignement américains à ne pas effectuer de collecte massive et indiscriminée de données personnelles. Néanmoins, il regrette le manque de garanties concrètes permettant d'éviter que de telles pratiques aient lieu.

Le G29 conclut : « *la première évaluation annuelle conjointe sera donc un moment clé permettant d'évaluer la robustesse et l'effectivité des garanties prévues par le Privacy Shield.* » et souhaite que la compétence des autorités de protection des données impliquées dans cette évaluation soit clairement définie. Lors de leur participation à la procédure d'évaluation, les représentants du G29 détermineront non seulement si des préoccupations demeurent mais également si les garanties proposées dans le cadre du bouclier vie privée sont effectives.

En second lieu, le président des États-Unis, M. Donald Trump vient de signer un décret [(1)] qui fragilise l'accord transatlantique en contredisant la politique menée sous la Présidence de Barack Obama en matière de renforcement de la protection des données personnelles.

En effet, après les révélations de M. Edward Snowden et la remise en cause de l'accord sur la Sphère de Sécurité, les États-Unis ont adopté en février 2016 une nouvelle loi relative aux recours juridictionnels [(2)], qui étend aux citoyens de certains pays – parmi lesquels ceux de l'Union européenne – les garanties dont bénéficient les citoyens et les résidents américains en matière d'utilisation des données personnelles par les agences fédérales en application de la loi sur la protection de la vie privée (*Privacy Act)* [(3)]. Par ailleurs, le Président Barack Obama, a signé, en 2014, une directive présidentielle [(4)] reconnaissant à

(1) Executive Order 13768, « Enhancing Public Safety in the Interior of the United States »*, 25 janvier 2017.*

(2) H.R.1428 - Judicial Redress Act of 2015-11-4th - Congress (2015-2016).

(3) La loi sur la protection de la vie privée encadre l'utilisation des données personnelles par les agences fédérales américaines – y compris les agences de renseignement et services de sécurité comme la NSA et le FBI – en prévoyant notamment pour les citoyens américains et les résidents permanents légaux, des droits d'accès, de rectification et de recours en cas d'utilisation illicite de leurs données. Sont prévues des exceptions en matière de sécurité nationale notamment.

(4) Presidential policy directive / PPD-28, 3, 17 janvier 2014.

toute personne, quelle que soit sa nationalité, un « droit légitime à la vie privée » et tentant d'encadrant de manière plus stricte la collecte de données par le renseignement américain.

Ces évolutions ont contribué à ce que la Commission européenne juge adéquat le niveau de protection des données personnelles aux États-Unis et l'adoption du bouclier vie privée.

Or, le décret signé par M. Donald Trump prévoit que les dispositions de la loi sur la protection de la vie privée relatives aux données personnelles ne s'appliqueront plus à ceux « *qui ne sont ni des citoyens des États-Unis ni des résidents permanents légaux* ». Un décret ne pouvant supplanter une loi, la loi relative aux recours juridictionnels (*Judicial Redress Act)*, qui concerne les citoyens européens, semble toujours applicable et le bouclier vie privée n'est pas directement remis en cause. Cependant, ce décret a fait naître des inquiétudes comme en témoignent les propos de la commissaire à la Justice, Mme Vera Jourová, qui a indiqué au site *EUObserver* qu'elle avait désormais « *besoin d'être certaine que le* Privacy Shield *subsistera* » compte tenu de la décision prise par le Président Donald Trump. (1) Le 15 février, le G29 a indiqué, dans un communiqué, qu'une lettre serait envoyée aux autorités américaines faisant état de ses inquiétudes et demandant une clarification sur l'impact du décret du président des États-Unis sur le *Privacy Shield*.

La Commission pourrait donc être amenée à remettre en cause cet accord, celle-ci étant compétente en application du paragraphe 5 de l'article 45 du règlement pour abroger, modifier ou suspendre la décision d'adéquation qu'elle a prise par voie d'actes d'exécution sans effet rétroactif « *lorsque les informations disponibles révèlent, en particulier à l'issue de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 de l'article 45* ».

De même, la Cour de justice de l'Union européenne pourrait remettre en cause le bouclier vie privée, comme elle l'a fait pour l'accord sur la Sphère de Sécurité, plusieurs associations, parmi lesquels *la Quadrature du Net*, ayant déposé un recours pour contester cet accord.

E. LE RENFORCEMENT DES AUTORITÉS DE RÉGULATION ET LA MISE EN PLACE D'UN GUICHET UNIQUE

1. L'évolution des missions des autorités de contrôle

Le renforcement des missions des autorités de contrôle intervient dans le cadre de la « *nouvelle ère dans la régulation* », suivant les termes de Mme Isabelle Falque-Pierrotin, présidente de la CNIL lors de son audition par la commission des

(1) « Trump's anti-privacy order stirs EU angst », *27 janvier 2017, https://euobserver.com/justice/136699*

Lois [(1)]. En effet, le règlement consacre un « *changement de paradigme* » pour les autorités de régulation en particulier et le traitement des données des personnes physiques en général. À la logique des formalités préalables est substituée une démarche de responsabilisation des acteurs et des droits des individus, dont le respect s'impose aux responsables de traitement et sous-traitants, qui peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Compte tenu de la suppression des formalités préalables, le contrôle *a priori* des traitements de données sera sensiblement simplifié : les responsables de traitements n'auront plus à effectuer de déclarations [(2)]. Les traitements les plus sensibles devront faire l'objet d'une étude d'impact sur la vie privée par les responsables de traitements, avant d'être soumis, dans certaines conditions, aux autorités de contrôle, afin qu'elles puissent, le cas échéant, s'opposer au traitement ou demander des garanties supplémentaires.

Celles-ci auront donc un rôle essentiel d'accompagnement des responsables de traitement, comme l'a rappelé Mme Isabelle Falque-Pierrotin lors de l'audition précitée : « *Le règlement européen marque une nouvelle étape dans la régulation concernant la protection des données personnelles. Il ne fait que confirmer une tendance que nous avions déjà anticipée en termes de changement de métier depuis quatre ans : de plus en plus, notre rôle est d'accompagner la mise en conformité des acteurs publics et privés*. » [(3)]

De même, dans les éléments transmis à la mission, la CNIL souligne l'importance du volet « mise en conformité » du règlement pour les autorités de contrôle qui devront répondre à de nombreuses demandes de conseils : « *Cette dimension de l'activité a connu une forte progression ces dernières années, et correspond plus aux mutations de l'univers numérique. Face à des technologies très évolutives, mais aussi aux enjeux de cybersécurité, les entreprises sont de plus en plus amenées à solliciter la CNIL " au fil de l'eau ", et à lui adresser des demandes de conseils. D'ores et déjà, la CNIL reçoit plusieurs milliers de demandes de conseils par an, et sa permanence téléphonique traite 140 000 appels par an de particuliers ou de professionnels.* »

Enfin, comme il a été évoqué précédemment, les autorités de régulation pourront **prononcer des amendes administratives** qui peuvent s'élever, selon la catégorie de l'infraction, **de 2 % à 4 % du chiffre d'affaires annuel mondial d'une entreprise**, et **à 10 ou 20 millions d'euros** pour les autres organismes (article 83 du règlement). Ces dispositions visent à renforcer l'effet dissuasif des sanctions que celles-ci peuvent prononcer, dont le niveau était jusqu'à présent modéré : ainsi jusqu'à la loi du 7 octobre 2016 pour une République numérique, la

---

(1) Audition de Mme Isabelle Falque-Pierrotin, Assemblée Nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 12 octobre 2016.

(2) 100 000 déclarations par an à la CNIL, mobilisant moins de deux équivalents temps plein travaillés.

(3) Audition du 12 octobre 2016.

CNIL ne pouvait prononcer que des amendes d'un montant maximum de 150 000 euros [(1)].

Ce montant des sanctions tient compte de l'évolution du poids économique des données personnelles et de l'importance économique qu'ont pris certains acteurs de l'économie numérique, pour lesquels une sanction de 150 000 euros n'était pas suffisamment dissuasive.

2. La mise en place de décisions conjointes des autorités de contrôle des États membres

a. Un interlocuteur unique pour les responsables de traitement

Les responsables de traitement ne rendront compte qu'à une seule autorité de contrôle au sein de l'Union européenne. Suivant une logique de guichet unique, ces organismes devront s'adresser à l'autorité de contrôle du pays où ils disposent de leur établissement principal, cette autorité étant alors désignée comme l'autorité « chef de file » (article 56 du règlement). Cet établissement principal étant entendu comme le lieu de leur siège central dans l'Union européenne ou de l'établissement au sein duquel sont prises les décisions relatives aux finalités et aux modalités du traitement de données (16 de l'article 4 du règlement).

Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles lorsqu'elles mettront en œuvre des traitements transnationaux.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), créé par l'article 68 du règlement, qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G 29.

(1) En 2014, la CNIL avait pu prononcer une sanction pécuniaire maximale de 150 000 euros à l'encontre de Google cf. https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-pecuniaire-de-150-000-eu-lencontre-de-la.

Le comité européen de la protection des données (CEPD)

L'article 68 du règlement prévoit que le CEPD est composé des chefs des autorités de contrôle de chaque État membre et du contrôleur européen de la protection des données, ou de leurs représentants respectifs. Le contrôleur est nommé pour un mandat de cinq ans renouvelable.

En application de l'article 70 du règlement, le CEPD :

– contrôle les activités de traitement de données à caractère personnel par l'administration européenne afin d'en vérifier la conformité avec les règles en matière de protection de la vie privée ;

– conseille les institutions et organes de l'Union européenne en ce qui concerne tous les aspects du traitement de données à caractère personnel, ainsi que les politiques et textes législatifs pertinents ;

– gère les plaintes et mène des enquêtes ;

– collabore avec les autorités nationales des pays de l'Union européenne pour assurer la cohérence dans le domaine de la protection des données ;

– suit l'évolution des technologies susceptibles d'avoir des incidences sur la protection des données.

L'activité courante du CEPD s'appuie sur deux grands services :

– l'entité « contrôle et mise en application », qui vérifie si les institutions et organes de l'Union européenne respectent les règles en matière de protection des données ;

– l'entité « politique et consultations », qui conseille les législateurs européens sur les questions de protection des données dans différents domaines d'action et sur les nouvelles propositions législatives.

b. Un mécanisme de décision conjointe des autorités de contrôle des États membres

Lorsqu'un traitement est transnational, le règlement a mis en place un mécanisme de décision conjointe des autorités de contrôle des États membres afin d'assurer une réponse unique sur l'ensemble du territoire européen et éviter ainsi la recherche des tribunaux les plus favorables (« *forum shopping* »).

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de **quatre semaines** pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas retenue, la question est portée devant le comité européen de protection des données (CEPD) qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ». L'autorité « chef de file » portera la décision ainsi partagée par ses homologues que le Comité européen de la protection des données soit ou non saisi. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union européenne.

La France, fortement soutenue par l'Allemagne [(1)], a souhaité ce mécanisme de guichet unique et de coopération entre les autorités de contrôle car cette organisation garantit :

– dans les cas transnationaux, que les personnes concernées conservent une proximité avec leur autorité de protection des données et leurs juridictions nationales, et que leur autorité de protection des données soit associée à la décision prise par l'autorité « chef de file » ;

– une prise de décision collective et mise en œuvre de façon uniforme sur le territoire européen, en associant toutes les autorités de protection des données concernées et en conférant au Comité Européen, doté de la personnalité juridique, le pouvoir d'adopter des décisions contraignantes pour régler les différends éventuels entre autorités de contrôle nationales. Ce Comité assurera l'uniformité et la cohérence de la jurisprudence et de la mise en œuvre du règlement dans l'Union européenne.

(1) Cette architecture a toutefois été fortement contestée par l'Irlande, la Belgique, le Royaume-Uni, la République tchèque, la Finlande et l'Espagne.

III. L'APPLICATION DU RÈGLEMENT À PARTIR DE MAI 2018 REND NÉCESSAIRE UNE ADAPTATION DU CADRE NATIONAL DE LA PROTECTION DES DONNÉES PERSONNELLES

Le règlement du 27 avril 2016 sera applicable à partir du 25 mai 2018, ainsi que le prévoit l'article 99. Il est donc nécessaire d'adapter préalablement le cadre législatif de la protection des données à caractère personnel, principalement défini par la loi du 6 janvier 1978. La loi pour une République numérique du 7 octobre 2016 a déjà modifié certaines de ses dispositions mais un travail plus vaste devra être mené lors de la prochaine législature. Parallèlement, la coopération entre les États membres et les travaux du G29 jouent un rôle essentiel pour préparer l'application du règlement.

• Les travaux de la Commission européenne et du G29

La Commission européenne, qui a la responsabilité de veiller à l'application du droit dérivé, en application de l'article 17 du traité sur l'Union européenne, suit déjà les travaux des États membres pour préparer l'application du règlement et la transposition de la directive sur les données policières et judiciaires. À cette fin, elle réunit mensuellement depuis le mois de septembre 2016 les experts nationaux chargés de ces travaux. Les réunions portent alternativement sur le règlement et la directive [(1)].

Les représentants de la Commission européenne rencontrés à Bruxelles par vos rapporteurs en janvier dernier leur ont indiqué qu'à ce stade, un dizaine d'États membres avaient finalisé un projet de loi.

Les réunions tenues jusqu'à présent sur le règlement ont notamment donné lieu à des discussions sur :

– les paragraphes 2 et 3 de l'article 6 permettant de maintenir ou introduire des dispositions spécifiques relatives aux traitements de données personnelles nécessaires au respect d'une obligation légale et aux traitements nécessaires 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 ;

– les conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information (article 8) ;

– les règles applicables aux traitements portant sur des catégories particulières de données, notamment les données de santé (article 9) ;

---

(1) Les agendas et les minutes de ces réunions sont publiés sur le site internet de la Commission européenne, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailPDF&groupID=3461.

– le délégué à la protection des données (article 37) ;

– les normes limitant certains transferts de catégories particulières de données (article 49) et les transferts non autorisés par le droit de l'Union européenne (article 48) ;

– les actions de groupe (article 80) ;

– le chapitre IX du règlement relatif aux situations particulières de traitement.

Par ailleurs, **la Commission européenne a entrepris la révision d'autres textes** afin de les mettre en conformité avec le règlement. Deux propositions législatives ont été publiées le 10 janvier dernier :

– une proposition de règlement devant se substituer à la directive de 2002 « vie privée et communications électroniques » ;

– une proposition de règlement relatif à la protection des données personnelles par les institutions et organes de l'Union européenne.

Elle a également publié une communication relative aux transferts internationaux de données personnelles.

Les propositions de la Commission européenne du 10 janvier 2017

La **proposition de règlement « vie privée et communications électroniques »** [(1)] vise à harmoniser les règles applicables aux communications électroniques avec les nouvelles normes contenues dans le règlement général sur le protection des données personnelles du 27 avril 2016.

Le champ d'application est élargi par rapport à la directive de 2002. La Commission prévoit que le règlement s'appliquera non seulement aux opérateurs de télécommunications traditionnels mais aussi à de nouveaux acteurs comme *WhatsApp*, *Facebook Messenger*, *Skype*, *Gmail*, *iMessage* ou *Viber* [(2)].

La protection de la vie privée portera sur le contenu des communications électroniques mais aussi sur les métadonnées (par exemple les données permettant d'identifier la source et la destination d'une communication, la date, l'heure et la durée d'une communication, sa localisation). Ces données devront être anonymisées ou effacées si l'utilisateur ne consent pas à leur traitement, sauf s'il s'agit de données nécessaires à la facturation.

Les utilisateurs devront avoir la possibilité de régler leurs paramètres sur leur navigateur de façon à accepter ou refuser les « cookies ».

Les communications non sollicitées seront interdites en l'absence d'accord de l'utilisateur. Le numéro du démarcheur ou un indicatif spécial indiquant qu'il s'agit d'un appel commercial devront apparaître.

Les autorités nationales de contrôle de la protection des données personnelles seront compétentes pour contrôler le respect du règlement.

La **proposition de règlement relatif à la protection des données personnelles par les institutions et organes de l'Union européenne**[(3)] renforce cette protection, afin de tirer les conséquences du règlement du 27 avril 2016.

Dans sa **communication sur les transferts internationaux de données personnelles**[(4)]**,** la Commission européenne annonce son intention de mener des discussions pouvant déboucher sur des décisions d'adéquation avec le Japon et la Corée en 2017, mais aussi l'Inde, ainsi que des pays d'Amérique latine et du voisinage européen. Lorsqu'il n'aura pas été possible d'adopter une décision d'adéquation, la Commission européenne souhaite utiliser d'autres instruments comme les clauses contractuelles standards ou les règles d'entreprise contraignantes.

(1) Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données personnelles dans le secteur des communications électroniques et abrogeant la directive 2002/58/CE (règlement vie privée et communications électroniques), COM (2017) 10 final, 10 janvier 2017.

(2) Commission européenne, communiqué de presse du 10 janvier 2017, IP-17-16_FR.

(3) Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes bureaux et agences de l'Union européenne et à la libre circulation de ces données et abrogeant le règlement CE 45/2001 et la décision 1247/2002/CE, COM (2017) 8 final, 10 janvier 2017.

(4) Communication de la Commission européenne au Parlement européen et au Conseil, « Échanger et protéger les données personnelles dans un monde globalisé », COM (2017) 7 final, 10 mai 2017.

Le G29, qui regroupe l'ensemble des autorités de protection des données des États membres et est présidé par Mme Isabelle Falque-Pierrotin, présidente de la CNIL depuis février 2014, est également fortement impliqué dans la mise en œuvre du règlement.

Le groupe a adopté le 2 février 2016 un plan d'action à cette fin [(1)], puis, en décembre 2016, des lignes directrices portant sur le statut et les missions des délégués à la protection des données, sur l'identification de l'autorité « chef de file » ainsi que sur le droit à la portabilité [(2)]. Il a également adopté des documents relatifs à l'assistance mutuelle, au guichet unique et aux opérations conjointes.

D'autres lignes directrices sont attendues en 2017 sur la certification ainsi que sur l'évaluation des risques et les analyses d'impact.

- **La préparation de l'application du règlement en France**

L'adaptation de notre législation relative à la protection des données est requise pour la mettre en conformité avec le règlement. Elle doit se traduire par **l'abrogation des dispositions incompatibles ou redondantes** – ce qui est l'effet classique d'un règlement – mais aussi par **l'adoption de dispositions nouvelles pour le compléter lorsqu'il ne peut s'appliquer directement**. Cela sera nécessaire en particulier en ce qui concerne la procédure de décision conjointe des autorités nationales de contrôle, prévue par l'article 60 mais qui appelle des précisions en droit national.

Interrogé par vos rapporteurs sur l'absence d'harmonisation des règles de procédure dans le règlement, le SGAE a indiqué que « *la diversité des législations nationales en matière de protection des données à caractère personnel et de sanction en cas de non-respect des obligations légales est telle qu'il était difficile de définir dans le règlement, de manière précise, les procédures applicables. En outre, l'ampleur et la complexité des négociations du règlement rendaient difficile de prévoir des règles détaillées permettant de procéder à une harmonisation également sur ces aspects*. »

À défaut d'une révision de la loi du 6 janvier 1978 avant le 25 mai 2018 précisant cette procédure, le nouveau régime de sanctions prononcées conjointement par les autorités de contrôle des États membres ne pourrait fonctionner, ainsi que l'a souligné Mme Isabelle Falque-Pierrotin, présidente de la CNIL, devant la commission des Lois [(3)]. L'interruption prochaine des travaux parlementaires jusqu'en juin 2017 imposera donc d'engager très rapidement ensuite la révision de la loi « Informatique et libertés » **afin que les travaux législatifs aboutissent avant la fin de l'année 2017**, compte tenu du temps nécessaire pour les éventuels décrets d'application.

---

(1) Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), 2 février 2016, 442/16/EN-WP 236.

(2) Cf. supra.

(3) Audition du 12 octobre 2016.

Dans ses réponses écrites au questionnaire des rapporteurs, la direction des affaires civiles et du Sceau (DACS) du ministère de la justice, chargée de la mise en conformité du droit national avec le règlement, indique qu'outre la loi du 6 janvier 1978, il sera nécessaire de modifier les différents textes législatifs évoquant des traitements de données à caractère personnel ou renvoyant à la loi de 1978 ainsi que le décret n° 2005-1309 pris pour son application. L'ampleur de ces modifications est en cours d'évaluation en lien avec les ministères concernés.

Dans la perspective du dépôt d'un projet de loi, la DACS a mis en place un groupe de travail associant le commissaire du Gouvernement auprès de la CNIL, des agents de la DACS, des représentants de l'administration de la CNIL, des universitaires, ainsi que des agents de la direction des affaires criminelles et des grâces (DACG), chargée de la transposition de la directive sur les données policières et judiciaires. La DACS sollicite également l'avis d'autres ministères sur des points particuliers les concernant. L'objectif est de parvenir à un projet de loi unique tirant les conséquences du règlement et transposant la directive.

Le III de l'article 65 de la loi pour une République numérique prévoit que le Gouvernement remet au Parlement, **au plus tard le 30 juin 2017**, un rapport sur les modifications de la loi de 1978 rendues nécessaires par l'entrée en vigueur du règlement. Compte tenu du calendrier précédemment évoqué, **vos rapporteurs jugent indispensable que la transmission de ce rapport et le dépôt du projet de loi révisant la loi du 6 janvier 1978 soient concomitants**.

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a pris en compte la problématique de la protection des données personnelles, sans pour autant couvrir l'ensemble du champ du règlement.

Les dispositions de la loi pour une République numérique relatives aux données personnelles

L'article 54 de la loi pour une République numérique consacre, à l'article 1er de la loi du 6 janvier 1978, un **droit à la libre disposition de ses données personnelles,** selon lequel « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». La reconnaissance de ce droit avait été recommandée par le Conseil d'État, dans son étude annuelle de 2014 (1), ainsi que par la commission de réflexion sur les droits et libertés à l'âge du numérique (2).

L'article 48 crée dans le code de la consommation un nouvel article L.224-42-1 selon lequel *« le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données. »* Ce nouveau **droit à la portabilité** sera applicable à partir du 25 mai 2018. S'agissant des données personnelles, le nouvel article L.224-42-2 renvoie au régime défini par l'article 20 du règlement (3). Pour les données n'ayant pas un caractère personnel, situées hors du champ du règlement, l'article L.224-42-3 définit un régime spécifique, ne s'appliquant qu'aux opérateurs de communication électronique.

L'article 63 introduit un « **droit à l'oubli numérique » pour les mineurs,** dans l'objectif d'anticiper l'application du règlement européen s'agissant des mineurs : *« sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci. »*.

Cette disposition ne concerne ainsi pas uniquement les mineurs mais la période pendant laquelle une personne était mineure, au titre de laquelle celle-ci peut demander l'effacement des données personnelles la concernant.

En cas d'absence de réponse ou de refus du responsable du traitement dans un délai d'un mois après la demande, la personne pourra saisir la CNIL qui devra se prononcer dans un délai restreint (trois semaines) suivant la date de réception de cette réclamation.

Les exceptions prévues sont identiques à celles énoncées à l'article 17 du règlement s'agissant du droit à l'effacement (4).

(1) Conseil d'État, Étude annuelle, « *Le numérique et les droits fondamentaux* », 2014.

(2) Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, op. cit.

(3) Cf. supra.

(4) Cf. supra.

Le même article définit également **le régime des données personnelles après le décès de la personne concernée (« mort numérique** »), sujet qui ne relève pas du règlement européen [(1)]. Selon le nouvel article 40-1 de la loi du 6 janvier 1978, toute personne peut donner des directives aux responsables de traitement quant à l'utilisation de ses données personnelles, après son décès. Ces directives peuvent concerner la conservation, l'effacement et la communication des données. Elles peuvent être générales ou particulières (propres à certains traitements). En l'absence de directives ou de mentions contraires des directives, les héritiers peuvent obtenir la clôture des comptes utilisateurs des défunts, s'opposer à la poursuite des traitements ou faire procéder à leur mise à jour.

L'article 57 modifie l'article 32 de la loi du 6 janvier 1978 afin de rendre obligatoire l'information par le responsable de traitement des personnes concernées sur la durée de conservation des données, ou en cas d'impossibilité, sur les critères utilisés pour déterminer cette durée.

L'article 58 créé un nouvel article 43 *bis* dans la loi du 6 janvier 1978 imposant aux responsables de traitement, « *lorsque cela est possible* », de permettre l'exercice par voie électronique des différents droits des personnes concernées par un traitement (droits d'accès, de rectification, d'opposition, d'information), dès lors que les données ont été recueillies par voie électronique. Cet article sera abrogé à compter du 25 mai 2018, l'exercice des droits étant régi par l'article 12, paragraphe 2, du règlement, d'application directe.

S'agissant enfin du **profilage**, l'article 4 crée un article L. 311-3-1 au sein du code des relations entre le public et l'administration, prévoyant que l'administration doit informer les intéressés lorsqu'une décision individuelle est prise sur le fondement d'un traitement algorithmique et leur communiquer, à leur demande, les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre, sous réserve des dispositions du 2° de l'article L. 311-5 relatives aux secrets protégés (par exemple le secret de la défense nationale, le secret relatif à la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations). La Commission d'accès aux documents administratifs (CADA), qui avait déjà jugé que les codes sources et les logiciels étaient des documents administratifs communicables, a précisé s'agissant de ce nouvel article, que « *pour présenter un effet utile, les dispositions du nouvel* [article] *doivent être comprises comme ouvrant aux personnes le droit d'obtenir de l'administration, en complément de la communication éventuelle du code source, dont la compréhension nécessite des compétences techniques en code informatique, des explications complémentaires, explicitant les règles de traitement mises en œuvre et les principales caractéristiques de celle–ci. Ces dispositions complètent ainsi, notamment en faveur des personnes morales, le droit que toute personne physique tient de l'article 39 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés d'obtenir du responsable d'un traitement de données à caractère personnel « les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.* » [(2)]

(1) Le considérant 27 du règlement précise que celui-ci ne s'applique pas aux données à caractère personnel des personnes décédées et que les États membres peuvent prévoir les règles relatives à ces données.

(2) CADA, Conseil n° 20155079 du 19 novembre 2015 sur le projet de loi pour une République numérique.

Les articles 59 et 60 de la loi ont élargi **les missions de la CNIL** :

– alors qu'il lui appartenait déjà de rendre un avis sur les projets de loi ou de décret relatifs à la protection des personnes à l'égard des traitements automatisés, sa consultation devient obligatoire sur les dispositions d'un projet de loi ou de décret relatives à la protection des données à caractère personnel ou à leur traitement ;

– il lui appartient désormais de mener une réflexion sur les questions éthiques et sociétales soulevées par l'évolution des technologies numériques ;

– elle se voit confier une mission de promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données ;

– elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de processus d'anonymisation des données à caractère personnel, notamment en vue d'une réutilisation d'informations publiques mises en ligne.

Par ailleurs, différentes dispositions de la loi organisent **la coopération de la CNIL avec des organismes extérieurs** :

– le président de la commission d'accès aux documents administratifs (CADA) ou son représentant siège à la CNIL et les deux autorités se réunissent dans un collège unique pour traiter de sujets d'intérêt commun, sur l'initiative conjointe de leurs présidents [(1)] ;

– la CNIL et l'Autorité de régulation des communications électroniques et des postes (ARCEP) peuvent se saisir mutuellement pour avis sur les questions relevant de leurs compétences respectives [(2)] ;

– la CNIL peut, à la demande d'une autorité de contrôle d'un État non membre de l'Union européenne, « *dès lors que celui-ci offre un niveau de protection adéquat des données à caractère personnel* » procéder à des contrôles et lui communiquer des informations, sous réserve d'avoir conclu une convention avec cette autorité [(3)] et à l'exception des traitements dits « de souveraineté ».

La loi a également renforcé **l'efficacité des procédures** de la CNIL. L'article 64 a modifié l'article 45 de la loi du 6 janvier 1978 afin de réduire le délai de mise en demeure de faire cesser un manquement, en cas « *d'extrême urgence* », de cinq jours à vingt-quatre heures. Lorsqu'un manquement ne peut pas faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte de la CNIL peut directement prononcer une sanction, après une procédure contradictoire.

(1) Articles 25 et 26 (articles 13 et 15 de la loi du 6 janvier 1978).

(2) Article 61 (article L. 135 du code des postes et des communications électroniques).

(3) Article 66 (article 49 bis de la loi du 6 janvier 1978).

Le I de l'article 65 modifie l'article 47 de la loi du 6 janvier 1978 afin de porter le **montant maximal des sanctions**, auparavant fixé à 150 000 euros, ou 300 000 euros cas de manquement réitéré du responsable de traitement à ses obligations, à **3 millions d'euros**. Il précise que la formation restreinte de la CNIL doit notamment prendre en compte « *le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission*. »

Il s'agit d'une **disposition transitoire**, le II de l'article 65 prévoyant qu'à compter du 25 mai 2018, les sanctions prononcées par la CNIL dans le champ du règlement le seront conformément à l'article 83 dudit règlement.

Vos rapporteurs tiennent à souligner l'importance de la réflexion sur l'usage des algorithmes et se félicitent des **avancées intervenues en France**, notamment du lancement par l'Institut national de recherche en informatique et automatique (INRIA) de la plateforme TransAlgo, évoqué lors de son audition par M. Daniel Le Métayer, directeur de recherche dans cet institut. Cette plateforme scientifique aura notamment pour objectif de vérifier et de tester les algorithmes de traitement de données et de favoriser la conception d'algorithmes responsables et transparents [(1)]. Cette initiative fait suite aux recommandations d'un rapport du Conseil général de l'économie sur la régulation des algorithmes [(2)].

Si certaines mesures d'adaptation requises par le règlement ne suscitent pas de débats, en revanche d'autres questions demeurent en suspens et devront être tranchées par le législateur.

A. DE NÉCESSAIRES ADAPTATIONS

1. Modifier le montant des amendes que peut prononcer la CNIL

L'article 65 de la loi pour une République numérique a relevé le montant des sanctions pécuniaires qui peuvent être prises par la CNIL en modifiant l'article 47 de la loi du 6 janvier 1978. Désormais la CNIL peut prononcer des amendes d'un montant de 3 millions d'euros, alors que ce montant était plafonné auparavant à 150 000 euros.

(1) INRIA, communiqué de presse du 1er décembre 2016, « Création d'une plateforme scientifique pour le développement de la transparence et de la responsabilité des algorithmes et des données « TransAlgo ».

(2) Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, Modalités de régulation des algorithmes de traitement des contenus*, établi par MM. Ilarion Pavel et Jacques Serris, 13 mai 2016.*

La loi précitée n'a pas aligné le montant des sanctions sur celui prévu par le règlement européen, celui-ci portant le montant maximal de sanctions à 20 millions d'euros ou 4 % du chiffre d'affaires mondial. Cependant, l'articulation entre l'article 47 précité et le règlement est expressément prévue au II de l'article 65 de la loi n°2016-1321 : « *II.-A compter du 25 mai 2018, les sanctions prononcées par la Commission nationale de l'informatique et des libertés dans le champ d'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE le sont conformément à l'article 83 dudit règlement. En dehors de ce champ, l'article 47 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant du présent article, est applicable.* »

Par ailleurs, selon les éléments transmis par la CNIL à la mission, le législateur devra aussi préciser le périmètre des sanctions sur plusieurs points :

– d'une part, le règlement européen ne limite pas le pouvoir des CNIL à des sanctions administratives, mais vise une série de mesures correctives. Le législateur devra donc déterminer si ces mesures peuvent être prises par l'autorité chargée de l'instruction (mise en demeure, mesure suspensive, saisine du juge) ou l'autorité chargée de la sanction ;

– d'autre part, le règlement ne prévoit de sanction administrative que pour les manquements à certaines dispositions du texte, et renvoie au droit national le soin de définir les sanctions des autres manquements. Il convient donc de déterminer si ces sanctions peuvent être administratives (comme c'est le cas aujourd'hui) ou peuvent prendre une autre forme (sanctions pénales notamment) ;

– enfin, se pose la question de la sanction de manquements à des obligations qui sont issues d'autres textes que le règlement, mais qui sont « connexes ». À titre indicatif, en vertu de la loi du 6 janvier 1978, la CNIL est compétente en matière de respect du droit d'opposition en matière de démarchage par voie électronique [(1)]. Il faudra donc « incorporer » dans le nouveau texte national remplaçant la loi du 6 janvier 1978 les sanctions de ces manquements, qui devront toutefois être proportionnés à celles retenues par les autres pays de l'Union.

2. Mettre en place une procédure de coopération en matière de sanction avec les autorités de contrôle des États membres

L'européanisation des procédures et des décisions change considérablement les conditions d'intervention de la CNIL en matière répressive.

(1) Article L 34-5 du code des postes et communications électroniques.

Si le règlement prévoit les mécanismes de coopération et de décision, il ne comporte aucune disposition sur les règles procédurales, qui relèvent de la seule compétence des États membres.

La diversité des législations nationales en matière de protection des données à caractère personnel et de sanction en cas de non-respect des obligations légales est telle qu'il était difficile de définir dans le règlement, de manière précise, les procédures applicables. En outre, l'ampleur et la complexité des négociations du règlement rendaient difficile de prévoir des règles détaillées permettant de procéder à une harmonisation également sur ces aspects.

Le règlement lui-même prévoit des cas où les amendes administratives n'existeraient pas : *« si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le présent article peut être appliqué de telle sorte que l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. »* (paragraphe 9 de l'article 83).

Il faut donc, dans toutes les lois nationales, concevoir des procédures qui permettent d'assurer la séparation des pouvoirs d'instruction et de sanction, mais aussi le respect des droits de la défense et du contradictoire.

Mme Falque-Pierrotin, présidente de la CNIL a rappelé l'enjeu de cette réforme lors de son audition par la commission des Lois : « *La procédure de sanction, actuellement fixée dans la loi informatique et libertés, doit être profondément revue à l'aune du règlement européen. Elle doit donc être ajustée avant mai 2018 pour que nous puissions, dès le 1er juin 2018, prendre des sanctions communes avec nos homologues européennes. Si l'une des autorités nationales européennes n'est pas prête au 1er juin 2018, le dispositif commun de sanctions ne pourra pas fonctionner*. » (1)

Deux types d'outils peuvent préciser les règles applicables en la matière :

– **les lignes directives adoptées par le G29**. Ce dernier a ainsi adopté des premières lignes directrices sur l'autorité chef de file, les étapes procédurales devant le comité européen de protection des données, l'articulation avec les autres procédures de coopération (assistance mutuelle et opération conjointe) parfois préalables à la production d'une décision conjointe, la nature des informations à échanger, les destinataires des informations ;

– **les dispositions nationales**.

Selon les éléments transmis par la CNIL à la mission, la loi devra prévoir trois cas de figure :

---

(1) Audition de Mme Isabelle Falque-Pierrotin, Assemblée Nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 12 octobre 2016.

– le cas où la CNIL est seule compétente (traitement de données mis en œuvre uniquement en France et ne concernant que des résidents sur le territoire français) ;

– le cas où le traitement concerne plusieurs pays européens dont la France et où l'établissement principal est situé en France, ce qui fait de la CNIL l'autorité « chef de file » ;

– le cas où le traitement concerne plusieurs pays européens dont la France et où l'établissement principal est situé dans un autre pays de l'Union, ce qui fait de la CNIL une autorité amenée à se prononcer sur les propositions de l'autorité chef de file.

Pour chacune de ces trois hypothèses, la loi – et subsidiairement le décret – devra définir :

– les modalités de contrôle opérationnelles sur le territoire français ;

– les modalités de contrôle conjoint, que la CNIL accueille des contrôleurs d'autres autorités ou qu'elle désigne des contrôleurs pour aller opérer des contrôles conjoints chez ses voisins européens. Cette disposition devra notamment fixer les procédures « d'incorporation » des contrôleurs des autres autorités dans les procédures nationales (habilitations, étendue des pouvoirs, etc.) ;

– les procédures d'échange d'information avec les autres autorités, selon que la CNIL est chef de file ou pas ;

– les procédures applicables devant la formation restreinte, et notamment les modalités de respect du principe du contradictoire dans un environnement de codécision : modalités de tenue de l'audience (invitation ou pas des homologues de la CNIL aux audiences de la formation restreinte), possibilité de recours à des services de communication électronique, etc ;

– les modalités de prise de décision (proposition de décision faite par la CNIL chef de file ; ou prise de position de la formation restreinte de la CNIL sur les propositions d'autres autorités ; communication d'une éventuelle objection pertinente et motivée) ;

– les modalités de notification et de représentation auprès du CEPD ;

– les modalités de publicité de la décision : le règlement européen ne prévoit pas la publicité de la décision et renvoie sur ce point aux États membres le soin de définir les éventuelles sanctions complémentaires.

– les modalités de notification, éventuellement après l'avis du CEPD.

B. DES QUESTIONS RESTENT EN SUSPENS

1. Une nécessaire clarification de certaines notions

Comme vos rapporteurs l'ont souligné précédemment, **plusieurs notions évoquées dans le règlement devront être clarifiées par le G29 afin de permettre une application uniforme du règlement parmi les États membres de l'Union européenne.**

C'est le cas notamment de la notion de « risque élevé » nécessitant qu'un responsable de traitement consulte l'autorité de contrôle avant de mettre en œuvre un traitement de données. L'article 35 du règlement prévoit que cette notion devra être précisée par les autorités de contrôle qui devront établir « *une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requis*e ». En outre, le G29 devrait adopter des lignes directrices au premier trimestre 2017 sur cette notion.

De même, devra être précisé dans quels cas un responsable de traitement devra informer les personnes concernées en cas de violation de données représentant un risque élevé pour sa vie privée.

Dans les éléments transmis à la mission, l'entreprise *Microsoft* souligne les risques d'applications divergentes d'un État membre à un autre. Il cite l'exemple de la nomination d'un délégué à la protection des données à caractère personnel qui *« sur la base des critères de l'article 37 pourrait s'avérer (…) incertaine pour des structures de petite dimension* » car quelles que soient les clarifications apportées par le G29 *« la notion de "*suivi régulier et systématique à grande échelle des personnes concernées *" ne sera pas d'interprétation uniforme et immédiate, notamment par les entités ne disposant pas des moyens et de l'expertise en protection des données requis pour procéder à un tel exercice.* »

Sur l'ensemble de ces notions, **vos rapporteurs considèrent que les avis du G29 seront essentiels pour éviter toute incertitude juridique potentiellement préjudiciable pour les responsables de traitement et pour les personnes concernées.**

Ils estiment également que la possibilité offerte par le règlement d'un regroupement d'entreprises, notamment les plus petites d'entre elles, pour désigner ensemble leur délégué à la protection de données, – qui est certes intéressante adossée au concept de « facilement joignable » – nécessitera néanmoins un travail très fin d'ajustement juridique.

2. Les règles spécifiques à certains types de traitements

Plusieurs dispositions du règlement prévoient que les États membres pourront maintenir ou adopter des règles spécifiques pour certains types de traitement. En réponse au questionnaire des rapporteurs, la DACS a indiqué qu'un

travail interministériel avait été engagé afin d'analyser si des modifications législatives seront nécessaires dans ces domaines spécifiques.

a. Les traitements des données de santé

L'article 4 du règlement définit les données de santé comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

L'article 9, paragraphe 1, dispose que les données de santé sont des données sensibles, dont le traitement est par principe interdit. Cependant, le paragraphe 2 prévoit que le traitement de ces données est autorisé dans différents cas, notamment :

– s'il est « *nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* » (g) ;

– s'il est *« nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé* [...] » (h) ;

– s'il est « *nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* » (i) ;

– s'il est « *nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* » (j).

Le paragraphe 4 dispose que « ***les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé*** ».

En droit national, l'article 8 de la loi du 6 janvier 1978 autorise :

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

– « *les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé* ».

L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a défini **un nouveau cadre d'accès aux données de santé médico-administratives à caractère personnel**, par l'introduction de dispositions symétriques dans le code de la santé publique et dans la loi du 6 janvier 1978.

L'article L. 1461-1 du code de la santé publique a créé un système national des données de santé (SNDS) rassemblant les différentes bases de données existantes en matière sanitaire et médico-sociale.

L'article L. 1460-2 dispose que les données du SNDS mises à la disposition du public « *sont traitées pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées y est impossible* ».

Le chapitre IX de la loi du 6 janvier 1978 (articles 53 à 61) définit le régime applicable aux traitements de données personnelles à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

L'article 54 prévoit que la CNIL autorise les traitements ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé, après avis du comité d'experts compétent [(1)]. Elle peut adopter des méthodologies de référence afin de simplifier la procédure pour les traitements les plus usuels.

La question de la compatibilité du nouveau régime défini par la loi du 26 janvier 2016 avec le règlement européen, dont l'adoption est postérieure, se posera lors de la discussion du projet de loi adaptant notre législation aux nouvelles normes européennes. Vos rapporteurs soulignent à cet égard que cette réflexion pourrait s'appuyer sur les travaux actuellement menés par la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS) sur l'accès aux données médicales personnelles détenues par l'assurance maladie.

M. Édouard Geffray, secrétaire général de la CNIL, auditionné par la MECSS, a indiqué que, dans le cadre du futur projet de loi, « *le Parlement devrait [...] se prononcer sur le point de savoir si nous conservons le dispositif issu de la*

(1) Si les recherches portent sur la personne humaine, le comité compétent de protection des personnes prévu à l'article L. 1123-6 du code de la santé publique ; dans les autres cas, le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (article L. 1451-1 du même code).

loi de modernisation de notre système de santé ou si nous remettons l'ouvrage sur le métier. Selon notre première analyse, le régime actuel pourrait demeurer, compte tenu du périmètre des exceptions prévues par le règlement européen – cette analyse doit cependant être affinée par la Direction des affaires civiles et du Sceau, qui pilote le projet au niveau interministériel. Je crains donc que le chantier ne soit pas totalement achevé, alors même que les décrets d'application de la loi de modernisation du système de santé ne sont pas encore publiés. » [(1)] .

b. Les traitements des données biométriques et génétiques

Comme les données de santé, les données biométriques et génétiques font partie des données sensibles dont le traitement est encadré par l'article 9 du règlement.

En droit national, le traitement automatisé de données comportant des données biométriques nécessaires au contrôle de l'identité des personnes est soumis à un régime d'autorisation préalable de la CNIL, en application de l'article 25 de la loi du 6 janvier 1978.

L'article 27 prévoit que les traitements de données personnelles mis en œuvre pour le compte de l'État et portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes doivent faire l'objet d'une autorisation par décret en Conseil d'État, pris après avis motivé et publié de la CNIL.

S'agissant des données génétiques, l'article 25 prévoit que « *les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements* » sont soumis à un régime autorisation de la CNIL.

Dans ses réponses écrites au questionnaire des rapporteurs, la CNIL a indiqué que ces régimes pouvaient s'entendre comme des « *conditions supplémentaires* » autorisées par l'article 9 du règlement et que le législateur pourrait choisir de les maintenir ou de les modifier.

c. Les traitements aux fins d'expression journalistique, artistique, universitaire et littéraire

L'article 85 du règlement dispose que « *les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire* » et « *prévoient des exemptions et dérogations* » aux chapitres II à IX « *si celles-ci sont nécessaires pour concilier le droit à la*

(1) Audition du 11 janvier 2017, compte-rendu n°8.

protection des données à caractère personnel et la liberté d'expression et d'information ».

La directive de 1995 prévoyait déjà des dérogations s'agissant de ce type de traitements, à l'exception de la finalité d'expression universitaire, ajoutée par le règlement.

En application de l'article 67 de la loi du 6 janvier 1978, les traitements mis en œuvre aux seules fins « *d'expression littéraire et artistique* » et « *d'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession* » sont dispensés du respect des obligations suivantes :

– la limitation de la durée de conservation des données ;

– l'interdiction de traiter des données sensibles ou des données relatives aux infractions, condamnations et mesures de sûreté ;

– les formalités de déclaration, à condition que le responsable du traitement désigne « *un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi* » ;

– les régimes d'autorisations pour les traitements statistiques, ceux concernant des données sensibles ou relatifs aux infractions, condamnations et mesures de sûreté ;

– l'information préalable des personnes concernées par le traitement ;

– le droit d'accès et le droit de rectification ;

– le transfert de données vers des États tiers.

Le dernier alinéa de l'article 67 précise que ces dérogations ne font pas obstacle à l'application des dispositions législatives relatives au droit de réponse et à la protection de la vie privée et de la réputation des personnes.

Dans leurs réponses écrites au questionnaire des rapporteurs, la CNIL comme la DACS ont estimé que le régime actuel avait permis d'atteindre un équilibre satisfaisant entre liberté d'expression et protection des données personnelles.

d. Les traitements de données relatives aux infractions, aux condamnations et aux mesures de sûreté

En application de l'article 10 du règlement, le traitement des données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peut être effectué que sous le contrôle de l'autorité

publique ou s'il est autorisé par le droit de l'Union ou le droit national, à condition que soient prévues des garanties appropriées pour les droits et libertés des personnes concernées. Un registre complet des condamnations pénales doit dans tous les cas être tenu sous le contrôle de l'autorité publique. Ces dispositions reprennent celles de la directive de 95/46.

En droit national, les traitements de données personnelles relatives aux infractions, aux condamnations et aux mesures de sûreté sont aujourd'hui encadrés par l'article 9 de la loi du 6 janvier 1978. Ces dispositions s'appliquent aux sanctions civiles et aux sanctions pénales (1) ainsi qu'à toutes les données qui, en raison des finalités du traitement automatisé, ne sont collectées que dans le but d'établir l'existence ou de prévenir la commission d'infractions, y compris par des tiers (2).

Outre les juridictions, les autorités publiques et les personnes morales gérant un service public, les autorités et personnes autorisées à traiter de telles données sont :

– les auxiliaires de justice (avocats à la Cour et aux Conseils, avoués, commissaires-priseurs, experts judiciaires, greffiers des tribunaux de commerce, huissiers de justice, notaires, syndics et administrateurs judiciaires) pour les besoins des missions qui leurs sont confiées par la loi ;

– les sociétés de perception et de réception des droits d'auteur et des droits d'artistes-interprètes, de producteurs de phonogrammes et de vidéogrammes ainsi que les organismes de défense professionnelle, afin de lutter contre la contrefaçon via internet ;

– les personnes traitant des données aux fins d'expression littéraire et artistique ou d'exercice de l'activité de journaliste.

En application de l'article 25, les traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sont soumis à un régime d'autorisation de la CNIL, à l'exception de ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées.

Le Conseil constitutionnel a précisé la portée des garanties des droits et libertés s'appliquant à ce type de traitement. Il a déclaré non conforme à la Constitution l'ouverture d'un droit de traitement de ces données par les personnes morales victimes d'infractions ou agissant pour leur compte pour les besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi (3). Le Conseil a estimé que, compte tenu de l'ampleur des traitements et de la nature des informations traitées, le législateur n'avait pas apporté suffisamment de

---

(1) Conseil d'État, 28 juillet 2014, Fathy X, *n° 262851.*

(2) Conseil d'État, 11 mai 2015, Société Renault Trucks, *n° 375669.*

(3) Conseil constitutionnel, décision n° 2004-499 DC 29 juillet 2004.

précisions (notamment les infractions concernées, un éventuel partage ou cession des données, la durée de conservation des données), celles-ci ne pouvant résulter des seules autorisations de la CNIL. Il a en revanche validé la dérogation visant les sociétés de droits d'auteur, compte tenu de l'objectif poursuivi et des garanties prévues par la loi.

e. Les traitements portant sur le numéro d'identification national

L'article 87 du règlement permet aux États membres de préciser les conditions spécifiques du traitement du numéro d'identification national « *ou de tout autre identifiant d'application générale* », sous réserve des garanties appropriées pour les droits et libertés de la personne concernée.

Les traitements de données à caractère personnel, mis en œuvre pour le compte de l'État ou d'une personne morale gérant un service public, portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (RNIPP), sont régis par l'article 27 de la loi du 6 janvier 1978.

Ces traitements relèvent de régimes d'autorisation [(1)], qui peuvent, selon les réponses de la CNIL à vos rapporteurs, se rattacher aux « *conditions spécifiques* » autorisées par le règlement ; ils pourraient donc être maintenus après le 25 mai 2018.

f. Les traitements des données personnelles à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques

L'article 89 du règlement donne aux États membres la possibilité d'autoriser des dérogations aux droits d'accès, de rectification, de limitation de traitement et d'opposition des personnes concernées lorsque des données personnelles sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou encore à des fins statistiques, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation de ces finalités. Par ailleurs, l'article 17, paragraphe 3, point d, prévoit que le droit à l'effacement ne s'applique pas s'agissant de ces traitements.

La loi du 6 janvier 1978 prévoit plusieurs dérogations pour ces catégories de traitements :

– ils sont exclus du champ d'application du droit à l'effacement des données personnelles collectées lorsque l'intéressé était mineur (article 40) ;

– les traitements dont la finalité se limite à assurer la conservation à long terme des documents d'archives sont dispensés des formalités préalables à leur mise en œuvre (article 36) ;

---

(1) Selon la nature des données et les finalités du traitement, par décret en Conseil d'État, par arrêté ou délibération de l'organe délibérant compétent, après avis motivé et publié de la CNIL.

– le respect des directives que toute personne peut définir relativement à la conservation, à l'effacement et à la communication de ses données personnelles après son décès est par ailleurs sans préjudice des dispositions applicables aux archives publiques (article 40) ;

– enfin, si toute personne physique a le droit d'interroger le responsable d'un traitement de données personnelles pour obtenir des informations sur celles de ces données qui le concerneraient ou encore les finalités dudit traitement, cette règle ne s'applique pas lorsque celles-ci sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et lorsque la durée du traitement n'excède pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique.

3. Les actions de groupe

L'action de groupe, introduite par la loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle [(1)], est ouverte lorsque plusieurs personnes physiques subissent un dommage ayant pour cause commune un manquement aux dispositions de la loi du 6 janvier 1978 et permet d'obtenir la cessation du manquement. La réparation des préjudices subis du fait de ce manquement fait, en revanche, l'objet d'une action individuelle classique.

Peuvent mener l'action :

– les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ;

– celles de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 411-1 du code de la consommation, lorsque le traitement de données à caractère personnel affecte des consommateurs ;

– les organisations syndicales représentatives de salariés, fonctionnaires ou magistrats lorsque le traitement affecte les intérêts de ces personnes.

Le paragraphe 1 de l'article 80 du règlement prévoit la possibilité pour les États membres d'adopter des dispositions nationales autorisant **des actions collectives avec mandat tendant à la réparation du préjudice subi**.

Selon les éléments transmis par la direction des affaires civiles et du sceau (DACS) du ministère de la Justice, la mise en œuvre d'une telle procédure ne constitue **qu'une possibilité donnée aux États membres** ainsi que l'indique clairement le considérant 142 du règlement : « *Lorsqu'une personne concernée estime que les droits que lui confère le présent règlement sont violés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association à*

(1) Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.

but non lucratif, constitué conformément au droit d'un État membre, (…) *pour qu'il introduise une réclamation en son nom auprès d'une autorité de contrôle, exerce le droit à un recours juridictionnel au nom de personnes concernées ou,* ***si cela est prévu par le droit d'un État membre****, exerce le droit d'obtenir réparation au nom de personnes concernées. Un État membre* ***peut prévoir*** *que cet organisme, cette organisation ou cette association a le droit d'introduire une réclamation dans cet État membre,* ***indépendamment de tout mandat*** *confié par une personne concernée, et dispose du droit à un recours juridictionnel effectif s'il a des raisons de considérer que les droits d'une personne concernée ont été violés parce que le traitement des données à caractère personnel a eu lieu en violation du présent règlement. Cet organisme, cette organisation ou* ***cette association ne peut pas être autorisé à réclamer réparation*** *pour le compte d'une personne concernée indépendamment du mandat confié par la personne concernée.* ». **La DACS considère donc à juste titre que le droit français est en conformité avec le règlement, dans une version minimale.**

Par ailleurs, les discussions au sein du groupe d'experts mis en place par la Commission européenne sur la mise en conformité du droit national au règlement ont abordé ce point le 2 décembre 2016. Il en ressort qu'en l'état de leurs réflexions, certains États membres n'envisagent pas de permettre un tel recours, d'autres mettront en œuvre un tel recours uniquement devant les tribunaux et non l'autorité de protection des données à caractère personnel, enfin certains permettront un tel recours devant leur autorité de protection des données.

Cette question devra donc être tranchée par le législateur, qui pourra décider de profiter de l'adaptation de notre législation pour élargir le champ des actions collectives. Vos rapporteurs notent que M. Édouard Geffray, secrétaire général de la CNIL, ainsi que de nombreuses personnes auditionnées par la mission, considèrent que l'extension du périmètre de l'action de groupe aux actions tendant à la réparation des préjudices subis, était souhaitable.

4. Le droit à la portabilité

L'article 48 de la loi du 7 octobre 2016 pour une République numérique prévoit la mise en œuvre, à compter du 25 mai 2018, d'un droit « *de récupération de l'ensemble de ses données* » pour le consommateur (article L. 223-42-1 du code de la consommation) [(1)].

Une distinction est faite selon le type de données concernées : s'agissant des données à caractère personnel, l'article L. 223-42-2 renvoie au régime défini par l'article 20 du règlement, qui s'applique à tous les responsables de traitement mais uniquement aux données fournies par les personnes concernées. Sur ce point, la loi nationale ne pouvait aller plus loin que le règlement européen, même si, ainsi que l'a indiqué Mme Aurélia Schaff dans ses réponses écrites à vos rapporteurs, la France aurait souhaité que celui-ci permette « *de consacrer un*

(1) Cf. supra.

droit à la portabilité plus ambitieux, qui permette aux personnes concernées de transférer plus facilement leurs données d'un responsable de traitement à un autre ».

S'agissant des données n'ayant pas un caractère personnel, l'article L. 223-42-3 définit un régime différent, ne concernant que les fournisseurs de service de communication au public en ligne. Ceux-ci devront proposer aux consommateurs une fonctionnalité gratuite leur permettant la récupération :

– de tous les fichiers qu'ils ont mis en ligne (*cloud computing*) ;

– « *de toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause* » ;

– et d'autres données associées au compte utilisateur du consommateur, non consultables en ligne mais facilitant le changement de fournisseur ou l'accès à de nouveaux services, qui seront définies par décret.

Ces deux régimes relèvent d'approches différentes, ainsi que l'a souligné M. Luc Belot, rapporteur du projet de loi : « *le règlement européen porte sur la protection des données personnelles, afin de renforcer la capacité des individus à exercer une maîtrise effective de l'usage des informations identifiantes. Le projet de loi, lui, porte sur le droit de la consommation qui vise à offrir des droits nouveaux au consommateur – personne physique ou morale – et sur le droit de la concurrence, qui cherche à réduire la viscosité du marché*. » [(1)]

Dans ses réponses écrites au questionnaire des rapporteurs, la DACS a précisé que les données n'ayant pas un caractère personnel visées par la loi sont les données anonymes au sens du règlement, c'est-à-dire les données ne contenant pas d'élément identifiant, qu'ils aient été supprimés ou qu'il n'y en ait jamais eu. Ces données étant situées hors du champ d'application du règlement, les deux régimes de portabilité sont, selon la DACS, compatibles. Elle ajoute que « *ces deux régimes semblent cohérents puisque, comme le précise l'article L.224-42-3 du code de la consommation modifié par l'article 48 de la loi pour une République numérique : « […]* ces données sont récupérées dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé *», là où l'article 20.1 du règlement (UE) 2016/679 indique «* dans un format structuré, couramment utilisé et lisible par machine ».

Cependant, vos rapporteurs soulignent que **la mise en œuvre de ces deux régimes risque de poser des difficultés d'interprétation**. En effet, les demandes de récupération de données aux opérateurs de communication électronique pourront concerner des données à caractère personnel. Il serait très complexe

(1) Rapport de M. Luc Belot, au nom de la commission des Lois, sur le projet de loi (n° 3318) pour une République numérique, n° 3399, 15 janvier 2016.

d'opérer un tri des données selon qu'elles ont un caractère personnel ou non. En outre, les critères différents définis par le règlement et par la loi (données fournies par la personne dans le règlement ; données résultant de l'utilisation du compte utilisateur n'ayant pas fait l'objet d'un « *enrichissement significatif* » par le fournisseur dans la loi) risquent d'être une source supplémentaire de confusion pour les opérateurs de communication électronique. **Ainsi que la CNIL l'a souligné dans ses réponses écrites, vos rapporteurs estiment donc qu' « *il conviendra sans doute d'harmoniser et de clarifier ces deux dispositifs afin que les professionnels connaissent exactement le champ de leurs obligations* »**.

5. Les dispositions spécifiques concernant les enfants

L'article 8 du règlement prévoit des règles particulières concernant le recueil du consentement des enfants s'agissant des services en ligne. Le consentement devra être recueilli auprès du titulaire de l'autorité parentale si l'enfant est âgé de moins de 16 ans, les États membres pouvant fixer par la loi un âge inférieur, ne pouvant pas être inférieur à 13 ans [(1)]. Néanmoins, vos rapporteurs estiment que les modalités de recueil de ce consentement sont incertaines, puisque l'article 8 prévoit que le responsable de traitement devra s'efforcer « raisonnablement » de vérifier la réalité du consentement du titulaire de l'autorité parentale. Ce point devrait faire l'objet d'une interprétation uniforme des États membres.

L'article 63 de la loi pour une République numérique a introduit un « droit à l'oubli numérique » pour les personnes qui étaient mineures au moment de la collecte des données. Cette disposition vise à anticiper l'application de l'article 17, paragraphe 1, point f, du règlement qui prévoit que les responsables de traitement devront effacer, sur demande des personnes concernées, les données qui « *[…] ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1*», c'est-à-dire les données collectées auprès d'enfants de 13 à 16 ans.

Cependant, la question de l'articulation de ces dispositions se pose en raison des âges différents fixés par le règlement (13 à 16 ans) et par la loi (18 ans) pour l'exercice du droit à l'effacement des données personnelles. Interrogée sur ce point par vos rapporteurs, la DACS a indiqué que « *bien que l'analyse de ces dispositions soit encore en cours, il ne semble pas à ce stade qu'il existe de problème de cohérence entre les dispositions du règlement et l'âge retenu dans la loi (18 ans) grâce à l'article 17.1 du règlement. Cet article évoque, en effet, six fondements légaux permettant l'effacement de la donnée à caractère personnel, le « droit à l'oubli ». Plus précisément, l'article 17.1(e) permet à un État membre de mettre en œuvre une législation spécifique à l'instar de la loi pour une République numérique*. »

(1) Cf. supra.

L'article 17, paragraphe 1, point e, permet d'obtenir l'effacement des « *[…]données qui doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis* » Selon l'interprétation étudiée par la DACS, cette disposition pourrait permettre de fixer une condition supplémentaire par rapport au règlement, telle que le prévoit la loi pour une République numérique s'agissant des mineurs âgés de 16 à 18 ans.

EXAMEN EN COMMISSION

Au cours de sa réunion du mercredi 22 février 2017, la commission des Lois procède à l'examen du rapport de la mission d'information.

M. le président Dominique Raimbourg. Nous passons maintenant à la présentation du rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française. Je vais donner la parole successivement à Mme Anne-Yvonne Le Dain, présidente et rapporteure, et à M. Philippe Gosselin, vice-président et co-rapporteur de la mission d'information.

Mme Anne-Yvonne Le Dain, rapporteure. Monsieur le président, mes chers collègues, la mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française qui nous a été confiée en novembre dernier comporte des enjeux essentiels en matière économique, mais aussi en termes de protection des personnes, sur cet espace extrêmement concret qu'est internet.

La directive du 24 octobre 1995 a constitué une première étape dans l'élaboration à l'échelon européen d'un cadre juridique d'ensemble relatif à la protection des données personnelles. Cette époque était celle de l'arrivée des combinés téléphone-fax-imprimante, mais aussi des premiers téléphones portables – des modèles qui pesaient alors plus d'un kilo. La considérable évolution technologique à laquelle on a assisté en vingt ans a eu des conséquences très importantes en matière économique, ainsi qu'en termes d'indépendance nationale et d'activité concrète des personnes physiques et morales sur les réseaux sociaux, qui se sont développés massivement au cours de ces dernières années.

La directive, élaborée dans le contexte des débuts d'internet, n'a donc pas pris en compte les évolutions technologiques majeures intervenues du fait de son développement. De plus, les marges de manœuvre laissées par le texte ont entraîné, en pratique, des différences substantielles dans les législations nationales à l'intérieur de l'Union européenne, ce qui n'est pas sans importance dans le contexte de compétition économique mondiale.

C'est pourquoi, compte tenu des évolutions du secteur, de sa force économique et de la nécessité de renforcer la protection offerte aux citoyens en la matière, la Commission européenne a souhaité, dès 2012, rénover le cadre existant afin de l'adapter aux nouvelles réalités du numérique. Après quatre ans de négociations lourdes, complexes, et ayant donné lieu à de nombreuses tergiversations, l'adoption du règlement général sur la protection des données, le 27 avril 2016 – sans doute sous l'influence de « l'affaire Snowden » – constitue l'aboutissement de cette volonté.

Ce règlement a été complété par une directive sur les données policières et judiciaires, ces deux textes constituant de fait le « paquet données personnelles ».

Le règlement du 27 avril 2016 sera applicable à compter du 25 mai 2018, date à laquelle la directive du 24 octobre 1995 sera abrogée. Il est donc nécessaire d'adapter préalablement notre cadre législatif, principalement défini par la loi du 6 janvier 1978, qui constitue le socle juridique de la protection des données personnelles en France et a été à l'origine de la création de la Commission nationale de l'informatique et des libertés (CNIL).

La loi du 7 octobre 2016 pour une République numérique, défendue au nom du Gouvernement par Mme Axelle Lemaire, a permis un renforcement significatif de la protection des données personnelles. Elle n'a pas cependant couvert l'ensemble du champ du règlement et une révision de la loi du 6 janvier 1978 est indispensable pour abroger les dispositions incompatibles ou redondantes et adopter des dispositions nouvelles répondant à l'évolution du paysage numérique et technologique en Europe et dans le monde.

Afin de préparer ces travaux législatifs, la commission des Lois a décidé, le 3 novembre 2016, la création d'une mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française. Compte tenu des délais restreints dans lesquels la mission d'information a mené ses travaux, nous avons fait le choix d'analyser en priorité l'impact du règlement, qui constitue le futur cadre général de la protection des données personnelles en Europe, donc en France.

De manière générale, la France a approuvé les objectifs d'approfondissement du cadre législatif de la directive du 24 octobre 1995 et de renforcement des droits des personnes concernées – contrairement à ce que l'on pourrait croire, cela n'est pas une évidence. Elle s'est opposée à toute disposition du règlement créant un recul par rapport au niveau de protection des droits des personnes tel qu'il était assuré jusqu'à présent par cette directive.

Elle s'est notamment montrée défavorable à l'établissement d'une catégorie distincte de données à caractère personnel pour les données pseudonymisées – ce qui a donné lieu à un vrai combat – et s'est opposée à l'application du critère de l'établissement principal pour déterminer quelle autorité de contrôle sera compétente en cas de traitement de données concernant les résidents de plusieurs États membres, afin d'éviter le phénomène de *forum shopping*, consistant, pour un demandeur, à choisir la juridiction du pays dont la loi lui est le plus favorable. Le règlement crée donc une instance de supervision européenne, indépendante de la Commission européenne et ayant une vocation supranationale pour régler les différends – ce qui constitue une avancée à mettre au crédit de la France et de l'Allemagne.

Le texte final est le résultat d'un compromis, mêlant des dispositions harmonisées à de multiples renvois aux droits nationaux – une cinquantaine, ce qui est beaucoup –, ce qui en fait un règlement *sui generis*. En dépit des nombreuses marges de manœuvre laissées aux États membres, le règlement constitue une véritable révolution en matière de protection des données personnelles, dont il ne faut pas sous-estimer la portée pour notre pays et nos concitoyens.

En effet, le règlement consolide les droits des personnes en renforçant les conditions applicables au consentement des personnes au traitement des données les concernant et en consacrant de nouveaux droits, comme le droit au déréférencement ou le droit à la portabilité. Cette avancée, très novatrice à l'échelle européenne, n'est pas simple à mettre en œuvre sur les plans technique et juridique : il y aura là beaucoup de travail, au cours des années qui viennent, pour les juristes comme pour les informaticiens.

Le règlement encadre également les conditions du recours au profilage, c'est-à-dire aux traitements de données personnelles visant à évaluer certains aspects personnels. Cette technique représente un risque pour la vie privée, qui ne doit pas être négligé.

Les actions collectives en matière de protection des données personnelles sont autorisées. Les États membres pourront prévoir dans leur droit national que ces actions peuvent tendre à la réparation du préjudice subi.

Par ailleurs, le règlement a un champ d'application élargi : le droit européen s'appliquera chaque fois qu'un résident européen, quelle que soit sa nationalité, sera directement visé par un traitement de données, y compris par internet ou par le biais d'objets connectés.

Alors que la directive du 24 octobre 1995 concerne essentiellement les responsables de traitements, le règlement européen « égalise » les obligations applicables aux sous-traitants et aux responsables de traitements, qui verront leur responsabilité conjointement engagée en cas de manquement à leurs obligations. Ce n'était pas le cas auparavant, ce qui exonérait les grandes sociétés de services informatiques de toute responsabilité en la matière.

Alors que la directive de 1995 reposait en grande partie sur l'existence de formalités préalables – déclaration, autorisations –, le règlement européen repose sur une logique de conformité et de responsabilité, dite d'*accountability*. L'idée est de faire en sorte que les institutions chargées de protéger les Français n'aient pas pour seule attribution de délivrer des autorisations, mais aussi d'accompagner le développement de l'économie, de manière à assurer la protection des personnes sans entraver l'activité économique.

La responsabilisation des entreprises est concrétisée par l'affirmation des principes de la « protection des données dès la conception » – *privacy by design* – et de « protection des données par défaut » – *privacy by default* –, qui imposent aux responsables de traitement de mettre en œuvre toutes les techniques nécessaires au respect de la protection des données personnelles, dès la conception du produit ou du service et par défaut. Nous sommes passés à une logique de prévention – chaque entreprise devra se demander si elle a fait tout ce qu'elle aurait dû ou pu faire pour assurer la protection de ses données –, ce qui constitue également une révolution.

Des analyses de l'impact des traitements sur la protection des données à caractère personnel devront être conduites par les responsables de traitement lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Si la notion de « risque élevé » n'est pas définie, elle constitue cependant une condition à laquelle les entreprises devront veiller.

Avec ce règlement, nous sommes en train de construire à l'échelle européenne un droit constituant une interface entre la *common law* anglaise et le droit romain, fondement de la législation française.

La désignation d'un délégué à la protection des données sera obligatoire d'une part dans le secteur public, d'autre part dans le secteur privé lorsque l'activité principale d'une entreprise concernera le suivi régulier et systématique des personnes à grande échelle ou le traitement à grande échelle de données sensibles ou relatives à des condamnations – comme on le voit, le critère retenu est celui de la puissance, du nombre de fichiers, de la masse de données.

Les responsables de traitement devront notifier les violations de données personnelles à l'autorité de contrôle, ainsi qu'aux personnes concernées en cas de risque élevé pour leurs droits et libertés. Le règlement prévoit des délais assez courts pour que les entreprises découvrant une faille de sécurité en informent l'autorité de contrôle et règlent le problème.

Le règlement donne aux autorités de contrôle la possibilité de prononcer des amendes administratives pouvant atteindre, selon la catégorie de l'infraction, 10 à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 % à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu : il est logique que, dans un secteur à forte valeur ajoutée, les amendes puissent atteindre des montants très élevés. Ces dispositions sont la manifestation de la puissance européenne.

Nous estimons qu'une attention particulière devra être accordée aux petites et moyennes entreprises, ainsi qu'aux entreprises naissantes, qui pourront rencontrer des difficultés pour respecter les nouvelles obligations posées par le règlement : en effet, il ne faudrait pas que le règlement empêche des TPE ou des PME d'émerger ou de se développer.

Enfin, ce règlement promeut l'affirmation d'une conception européenne de la protection des données personnelles, différant de celle promue notamment par les États-Unis. Comme l'ont rappelé plusieurs personnes entendues par la mission, cette conception, qui pourra paraître *a priori* contraignante pour les acteurs du numérique, constitue une opportunité de faire de l'Union européenne un espace où les entreprises, quelle que soit leur taille, pourront faire valoir la protection des données personnelles comme un avantage compétitif et non comme une restriction de leurs libertés. Si les personnes physiques sont souvent friandes de modernité, elles n'en sont pas moins attachées au respect de leur intimité.

L'Union européenne représente un marché de consommateurs important, notamment en matière de pouvoir d'achat, dans le domaine du numérique : il ne s'agit donc pas seulement d'un enjeu de protection des données des résidents européens, mais également d'un enjeu économique et technologique. Au sein de l'Europe, mais aussi à l'échelle du monde, il faut absolument que la France sache prendre la place qui lui revient au cours des années à venir.

Cependant, cette différence de conception entre les États-Unis et l'Union européenne n'est pas sans conséquence sur les transferts de données des usagers européens vers les entreprises américaines. En effet, si le règlement autorise les responsables de traitement et les sous-traitants à transférer des données hors de l'Union européenne, ce n'est que dans la mesure où ces transferts garantissent un niveau de protection suffisant et approprié des données personnelles. En la matière, il faudra donc faire preuve d'une vigilance particulière.

La Cour de justice de l'Union européenne a, par un arrêt *Schrems* du 6 octobre 2015, invalidé la décision de la Commission européenne constatant que les États-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées et permettant l'application de l'accord conclu entre les États-Unis et l'Union européenne, appelé « Sphère de sécurité » ou *Safe Harbor*. À la suite de cet arrêt, la Commission a conclu en février 2016 un nouvel accord avec les États-Unis portant sur le cadre des transferts transatlantiques de données, le « bouclier vie privée Union européenne-États-Unis » – *EU-US Privacy Shield*.

Or la pérennité de cet accord pourrait être remise en question dans les mois qui viennent, compte tenu : de certaines réserves émises sur celui-ci par le groupe qui rassemble les « CNIL » des États membres – appelé G29 – ; de la remise en cause par le président américain Donald Trump – notamment par le décret adopté le 25 janvier 2017 – des garanties accordées aux citoyens de l'Union européenne en matière de protection des données personnelles sous la présidence de Barack Obama ; enfin du recours déposé par plusieurs associations contre cet accord devant la Cour de justice de l'Union européenne.

Le monde occidental se trouve donc à un moment de son histoire où il doit faire face à une situation compliquée, ce qui nous ouvre un espace de travail considérable dans les mois et les années à venir si l'on veut éviter que la question de la protection des données personnelles des résidents européens ne soit instrumentalisée par les États-Unis et leur président.

M. Philippe Gosselin, co-rapporteur. Monsieur le président, mes chers collègues, le rapport qu'Anne-Yvonne Le Dain et moi-même vous présentons aujourd'hui a effectivement été rédigé dans des conditions particulières, notamment dans des délais très courts.

L'application du règlement à partir de mai 2018 rend nécessaire une adaptation du cadre national de la protection des données personnelles, principalement défini par la loi du 6 janvier 1978, dite « Informatique et libertés », qui a été à l'origine de la création de la CNIL, l'une des toutes premières autorités administratives indépendantes, et un modèle pour celles qui ont été créées ultérieurement.

À la différence de la directive, qui doit faire l'objet d'une transposition, le règlement est en principe applicable immédiatement en droit national. Le règlement qui nous intéresse est un peu particulier, dans la mesure où il nécessite quelques mesures de transposition – si je devais user d'un néologisme, je dirais qu'il s'agit d'une « régletive ».

L'interruption prochaine des travaux parlementaires imposera d'engager dès le début de la nouvelle législature la révision de la loi du 6 janvier 1978 et, nonobstant le principe de séparation des pouvoirs, nous devrons veiller à ce que le Gouvernement dépose un projet de loi dès juin 2017, en tout état de cause avant l'été, afin que les travaux législatifs puissent aboutir avant la fin de l'année 2017, compte tenu du temps nécessaire pour publier les décrets d'application et pour que le texte soit applicable en droit français avant le 25 mai 2018.

La loi du 7 octobre 2016 pour une République numérique a pris en considération la problématique de la protection des données personnelles, sans pour autant couvrir l'ensemble du champ du règlement. Certaines de ses dispositions visent à anticiper l'application du règlement – je pense au droit à l'oubli numérique pour les mineurs, une disposition qui avait fait l'unanimité –, tandis que d'autres ont été adoptées à titre transitoire – c'est le cas du renforcement des sanctions prononcées par la CNIL – ou traitent de sujets connexes – par exemple, les données des personnes décédées, ou la portabilité des données n'ayant pas un caractère personnel.

Nous avons distingué, dans le rapport, deux catégories de mesures : d'une part, les adaptations nécessaires, qui ne devraient pas donner lieu à des débats très approfondis, d'autre part, les questions restant en suspens, qu'il reviendra au législateur de trancher en faisant usage de sa faculté d'appréciation, voire d'opportunité.

La future loi devra adapter les dispositions relatives aux sanctions pouvant être prononcées par la CNIL. Si la loi pour une République numérique a d'ores et déjà prévu qu'à compter du 25 mai 2018, les sanctions entrant dans le champ du règlement seront celles prévues par ce dernier, d'autres évolutions seront nécessaires. Le législateur devra notamment définir les procédures s'appliquant aux mesures correctives pouvant être prises par la CNIL – mise en demeure, mesure suspensive, saisine du juge –, ainsi que les sanctions des manquements ne relevant pas du règlement.
Par ailleurs, si le règlement prévoit les mécanismes de coopération et de décision des autorités nationales de contrôle, il ne comporte aucune disposition sur les règles

procédurales, qui relèvent de la seule compétence des États membres. Les lignes directrices adoptées par le G29 – dénommé ainsi en référence à l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci, et ayant vocation à se transformer en une force institutionnelle à compter de l'entrée en vigueur du règlement – sur ces questions devraient donner un cadre au législateur.

Par ailleurs, d'autres questions restent en suspens. Il s'agit tout d'abord de l'interprétation de certains concepts. Plusieurs notions évoquées dans le règlement devront être précisées afin de permettre une application uniforme de ce texte au sein de l'Union européenne. C'est le cas, par exemple, de la notion de « risque élevé », nécessitant qu'un responsable de traitement consulte l'autorité de contrôle avant de mettre en œuvre un traitement de données, sujet sur lequel tous les États n'ont pas la même perception ni la même sensibilité. Sur l'ensemble de ces notions, nous considérons que les avis du G29 seront essentiels pour éviter toute incertitude juridique potentiellement préjudiciable aux responsables de traitement dont la responsabilité pourrait être engagée et aux personnes concernées.

Comme l'a dit Mme Anne-Yvonne Le Dain, nous devrons également prévoir des dispositions afin d'éviter la pratique par les entreprises du *forum shopping*, qui se ferait à leur avantage mais au détriment de l'intérêt collectif – tout en veillant à ne pas corseter trop fortement le dispositif, afin que, si des marges de manœuvre existent, elles bénéficient à l'implantation d'entreprises en France : il ne faudrait pas que notre pays devienne un repoussoir.

Ensuite, plusieurs dispositions du règlement prévoient que les États membres pourront maintenir ou adopter des règles spécifiques pour certains types de traitement.

Pour ce qui est des données de santé, un sujet plus sensible en France que dans d'autres États, la question de la compatibilité avec le règlement européen du nouveau régime d'accès aux données de santé médico-administratives à caractère personnel, défini par la loi de modernisation de notre système de santé du 26 janvier 2016, se posera sans aucun doute. Le caractère très récent de cette réforme – tous les décrets d'application n'ont pas encore été publiés – et les travaux actuellement en cours de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS) sur cette question nous ont conduits à ne pas aborder ce sujet en détail.

D'autres traitements font l'objet de règles spécifiques définies par la loi du 6 janvier 1978. Il s'agit notamment des données biométriques et génétiques, des traitements aux fins d'expression journalistique, artistique et littéraire, des traitements de données relatives aux infractions, aux condamnations et aux mesures de sûreté, des traitements portant sur le numéro d'identification national (NIR) – une question sur laquelle la CNIL a une doctrine constante depuis près de quarante ans, dans le souci d'éviter que ce numéro n'agrège trop d'éléments sur un individu donné –, des traitements à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques. D'après les éléments qui nous ont été communiqués par la CNIL, ces règles spécifiques devraient pouvoir être maintenues dans le cadre des marges ouvertes par le règlement. Il nous appartiendra de faire en sorte que les dispositifs des différents États ne divergent pas trop.

La question d'un éventuel élargissement du champ de l'action de groupe devra être tranchée par le législateur. L'action de groupe en matière de protection des données personnelles a été introduite par la loi du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle. Elle est ouverte lorsque plusieurs personnes physiques subissent un

dommage ayant pour cause commune un manquement aux dispositions de la loi du 6 janvier 1978 et permet d'obtenir la cessation du manquement.

Le règlement prévoit la simple possibilité pour les États membres d'adopter des dispositions nationales autorisant des actions collectives avec mandat tendant à la réparation du préjudice subi. Plusieurs personnes entendues par la mission ont estimé qu'il serait souhaitable de permettre ce type d'actions de groupe pour aller jusqu'au bout de la logique du règlement. Nous aurons également à nous prononcer sur ce point.

La loi pour une République numérique prévoit la mise en œuvre, à compter du 25 mai 2018, d'un droit à la portabilité de l'ensemble de ses données pour le consommateur – c'est-à-dire du droit de changer d'opérateur sans difficulté particulière. En ce qui concerne les données personnelles, elle renvoie au régime défini par l'article 20 du règlement. Les données non personnelles relèvent, elles, d'un régime différent, ne s'imposant qu'aux opérateurs de communications électroniques. Nous estimons que la mise en œuvre de ces deux régimes risque de poser des difficultés d'interprétation et souhaitons que ceux-ci puissent être clarifiés et mieux articulés dans le cadre de la future loi.

Enfin, la question de l'articulation des dispositions nationales et du règlement se pose à l'égard des dispositions spécifiques aux mineurs. En effet, des âges différents sont fixés par la loi pour une République numérique – dix-huit ans – et par le règlement – seize ans, pouvant même être abaissés jusqu'à treize ans par le droit des États membres – pour l'exercice du droit à l'effacement des données personnelles.

Cependant, selon une interprétation avancée par le ministère de la justice, une disposition de l'article 17 du règlement, rendant obligatoire l'effacement des données pour respecter une obligation légale définie par le droit national, pourrait permettre de fixer une condition supplémentaire par rapport au règlement, comme le prévoit la loi pour une République numérique pour les mineurs âgés de 16 à 18 ans.

En conclusion, nous avons souhaité, par ce travail, appeler votre attention sur les enjeux posés par l'application du règlement. Nous avons également voulu transmettre un témoin à la future assemblée, qui devra examiner le projet de loi de révision de la loi du 6 janvier 1978 dans un délai très bref – pour compléter ce que j'ai dit tout à l'heure au sujet du calendrier, j'ajouterai qu'il serait souhaitable de désigner un rapporteur et un rapporteur d'application durant la session extraordinaire de juillet, afin que les auditions puissent démarrer dès septembre, c'est-à-dire avant l'examen des lois de finances.

En cette fin de législature, nous n'avons pas eu la prétention de trancher toutes les questions, mais plutôt le souci d'apporter des éléments utiles au débat sur ce sujet essentiel pour la protection des droits et libertés.

Mme Anne-Yvonne Le Dain, rapporteure. Je précise que le règlement contient une série de notions extrêmement importantes : la portabilité, le déréférencement, l'anonymisation, le consentement, le profilage, la réparation, la responsabilité, la sous-traitance, la notion de prévention, celle d'impact, celle de risque élevé, la nécessité d'informer l'autorité de référence dans un délai court, le concept de dialogue et celui d'obligation faite aux entreprises de prévoir le risque. Toutes ces notions comportent une marge d'interprétation importante. Il est donc essentiel que la France, au cours de la prochaine législature, construise autour de ce vocabulaire un dispositif qui serve à la fois son économie et l'intérêt de ses citoyens.

M. Guillaume Garot. Je veux saluer la précision et la qualité du rapport qui vient de nous être présenté ce matin. La problématique a été bien posée : comment peut-on garantir et améliorer la protection des libertés individuelles ? Je voudrais revenir sur le dernier point qu'a évoqué le rapporteur sur l'effacement des données concernant les enfants : dix-huit ans dans la loi pour la République numérique ; entre treize et seize ans dans le règlement européen. Vous présentez une solution d'interprétation juridique. À votre avis, peut-on aller plus loin et dans quelle direction ?

Mme Sophie Dion. Pour ma part, je voudrais poser une question sur le droit à l'oubli. À la lecture du rapport, j'ai cru comprendre que ce droit ne concernait que les mineurs. Dans quelle mesure et selon quel régime juridique pourrait-il être étendu au-delà de la minorité ? S'agissant de l'action de groupe, j'avoue que je n'ai pas très bien compris comment les choses pouvaient s'articuler avec le règlement.

M. Philippe Gosselin, co-rapporteur. Le ministère de la justice est le chef de file des travaux en cours sur la question des mineurs. Sous réserve d'un examen juridique plus approfondi, il semble que l'article 17 pourrait permettre aux États membres d'ajouter une condition supplémentaire pour pouvoir « coller », si je puis dire, à l'âge réel de la majorité. Quoi qu'il en soit, je pense ne trahir aucune sensibilité en disant que l'objectif est d'arriver à graver réellement cet âge de dix-huit ans, nonobstant des évolutions sur d'autres sujets dont on ne va pas enclencher la discussion à l'instant précis. Fixée à l'âge de dix-huit ans en France, la majorité entraîne un certain nombre de conséquences. Notre objectif collectif est bien de conserver l'âge de dix-huit ans et de mettre notre droit en adéquation avec le règlement européen. Notre volonté est claire ; les moyens d'y parvenir semblent être clairs aussi mais ils restent à affiner.

Mme Anne-Yvonne Le Dain, rapporteure. En ce qui concerne le droit à la réparation, le principe est posé par le réglement. Il est également dit que les États peuvent fixer une amende. Ce n'est pas du tout anodin. Il existe également des marges d'interprétation à la discrétion de chacun des pays. Il faut quand même avoir en tête que l'objectif est de construire un droit européen puissant pour construire une Europe de puissances, notamment dans ces champs qui sont en expansion économique.

La France et l'Allemagne, qui ont beaucoup en commun, sont deux pays très présents dans le groupe du G29. Les pays européens doivent constituer progressivement un système qui empêche le fameux *forum shopping*. D'où l'importance de cette autorité nouvelle, créée par le règlement et indépendante de la Commission, qui pourrait être une instance d'arbitrage dans le cas où une entreprise serait implantée dans plusieurs pays. La France et l'Allemagne ont pesé pour qu'il y ait une décision conjointe des autorités de contrôle concernées, c'est-à-dire pour que, par exemple, l'Irlande ne puisse pas décider pour tout le monde au prétexte que les données seraient dans ce pays. Ce combat n'a pas été facile mais il a été gagné. On peut considérer que tout cela est une source d'inquiétude mais c'est tout simplement le monde vers lequel on va.

M. Philippe Gosselin, co-rapporteur. L'action de groupe, introduite dans la loi du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle, permet de mettre fin aux manquements commis par les responsables de traitement. En revanche, il manque dans ce texte le second étage de la fusée : le droit à réparation. Le règlement européen, lui, permet à la fois de mettre fin aux manquements et d'envisager la réparation. La question de l'intégration du droit à réparation dans notre législation interne, qui s'est posée lors de nos débats sur l'action de groupe, ressurgira en raison de ce règlement européen.

Mme Anne-Yvonne Le Dain, rapporteure. Le règlement actuel prévoit de lourdes amendes : 10 à 20 millions d'euros, et entre 2 % et 4 % du chiffre d'affaires de l'entreprise. Rappelons que l'amende infligée à Google par la CNIL était de 150 000 euros, une somme dérisoire. Les montants prévus par le règlement européen modifient l'équation mentale de celui qui veut jouer avec le droit.

M. Philippe Gosselin, co-rapporteur. Ces montants concernent d'autres types de manquements que les actions de groupe.

M. le président Dominique Raimbourg. S'il n'y a pas d'autres interventions, nous allons procéder au vote. Vous allez devoir dire, mes chers collègues, si vous êtes d'accord pour que le rapport soit publié et qu'il serve ainsi de base aux travaux concernant la loi qui sera débattue lors de la prochaine législature. Nous avons jusqu'au mois de mai 2018 pour élaborer ces nouvelles règles.

M. Philippe Gosselin, co-rapporteur. Nous devons le faire avant : le 25 mai 2018 est la date d'entrée en vigueur du règlement. Les règles que nous aurons élaborées devront donc être promulguées en janvier 2018, au plus tard, afin que les décrets d'application puissent être pris et qu'il n'y ait aucun vide juridique.

Mme Anne-Yvonne Le Dain, rapporteure. En clair, il faut démarrer dès le mois de juin et que la navette parlementaire soit terminée à Noël.

La commission des Lois ***autorise*** *à l'unanimité la publication du rapport d'information.*

PERSONNES ENTENDUES PAR LA MISSION [1]

- Mme Aurélia Schaff, conseillère, cheffe du secteur Espace judiciaire européen au Secrétariat général des Affaires européennes (SGAE), Mme Ève Jullien, adjointe aux conseillères judiciaire et juridique, chargée de la protection des données personnelles, et Mme Lorraine Simonnet, adjointe à la conseillère juridique chargée du suivi de la transposition des directives

- M. Edouard Geffray, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL) et Mme Tiphaine Inglebert, conseillère pour les questions institutionnelles et parlementaires

- M. Henri Verdier, directeur de la direction interministérielle des systèmes d'information et de communication (DINSIC) et M. Périca Sucevic, conseiller juridique

- M. Daniel le Métayer, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA)

- M. Philippe Aigrain, président et Mme Léa Caillère Falgueyrac, analyste juridique et politique de l'association La Quadrature du Net

- M. Jean-Christophe Gracia, chef de service, adjoint à la directrice des affaires civiles et du Sceau du ministère de la Justice, MM. Romain Felsenheld, chef du bureau du droit constitutionnel et du droit public général, Corentin Hellendorff, rédacteur au bureau du droit constitutionnel et du droit public général et Emmanuel Laforêt, adjoint au chef de bureau

- M. Winston Maxwell, avocat associé au cabinet Hogan Lovells

- Mme Célia Zolynski, professeure de droit à l'université de Versailles-Saint-Quentin-en-Yvelines, et M. Romain Delassus, rapporteur général, du Conseil national du numérique (CNNum)

- MM. Éric Barbry, administrateur et président de la commission juridique, et Nicolas Herbreteau, administrateur de l'Association de l'économie numérique (ACSEL) et Mme Céline Avignon, avocate

- Mme Marie-Blanche Niel-Gilly, directrice des données personnelles et correspondante Informatique et Libertés, M. Maxime Duclaux, responsable des relations institutionnelles et Mme Clara Hanot, chargée des affaires publiques de la société SoLocal Group

- M. Alexandre Tisserant, directeur adjoint du cabinet de Mme Axelle Lemaire, secrétaire d'État auprès du ministre de l'Économie et des Finances, chargée du numérique et de l'innovation, Mme Chantal Rubin, adjointe à la direction générale des entreprises et Mme Julie Wable, membre du cabinet

(1) Liste présentée par ordre chronologique.

- M. Massimo Bucalossi, vice-président de la commission « Intranet et nouvelles technologies » du Conseil national des Barreaux, et Mme Laurence Dupont, juriste, référente CNIL

- M. Éric Le Quellenec, avocat, vice-président de l'Union des jeunes avocats de Paris, et Mme Marie-Hélène Fabiani, avocate, responsable de la commission « Nouvelles technologies »

- M. Dominique Guibert, président de l'Association européenne des droits de l'homme (AEDH) et Mme Maryse Artiguelong, membre du bureau exécutif et responsable du groupe de travail protection des données

- M. Marc Mossé, directeur des affaires publiques et juridiques Europe de Microsoft, Mme Marie-Charlotte Roques-Bonnet, directrice de la politique de confidentialité et M. Jean-Renaud Roy, directeur des affaires publiques France

DÉPLACEMENT À BRUXELLES

18 janvier 2017

Contrôleur européen de la protection des données

– M. Giovanni Butarelli, contrôleur européen de la protection des données

Commission européenne

– M. Kevin O'Connell, membre du cabinet de Mme Věra Jourová, commissaire chargée de la justice, des consommateurs et de l'égalité des genres

– Mme Irina Vasiliu, unité protection des données de la direction générale chargée de la justice et des consommateurs

Digital Europe

– M. Patrice Chazerand, directeur

– M. Alexander Whalen, gestionnaire principal des politiques

ANNEXE N° 1 : LISTE DES RENVOIS AU DROIT NATIONAL PRÉVUS PAR LE RÈGLEMENT 2016/679

1) Pour les règles sectorielles spécifiques des Etats membres, notamment pour les données sensibles et les conditions de licéité, et la marge de manœuvre des Etats membres : *considérant 10*
2) Pour la prise en compte des besoins spécifiques des TPE/PME : *considérant 13*
3) Pour adapter le règlement pour le secteur public, y compris pour adopter des conditions spécifiques ou des restrictions : *considérant 19* ; article 6, paragraphe 2
4) Pour désigner certains responsables de traitement : article 4, point 7 ;
5) Pour les traitements de données par les juridictions et la supervision de ceux-ci : *considérant 20*
6) Pour les données des personnes décédées : *considérant 27)*
7) Pour les tiers autorisés : *considérant 31* et article 4, point 9 ;
8) Pour la licéité des traitements du secteur public (dans l'intérêt public ou imposant une obligation légale) et la création de tels traitements : *considérants 45, 47*; article 6, paragraphe 3 ;
9) Pour déterminer la compatibilité, la licéité et la base légale des traitements de données ultérieurs dans l'intérêt public : *considérants 50, 51*; article 6, paragraphe 4 ;
10) Pour les conditions relatives au consentement des enfants de moins de 16 ans et de plus de 13 ans : article 8, paragraphe 1er ;
11) Pour les traitements de données sensibles, y compris de santé, génétiques ou biométriques : *considérants 51, 52, 53*, article 9, article 17 pour les limitations au droit à l'oubli et 21, paragraphe 6 pour les traitements de données sensibles à des fins scientifiques, statistiques ou historiques dans l'intérêt privé ;
12) Pour le traitement des données relatives aux condamnations pénales : article 10 ;
13) Pour déterminer les conséquences de demandes d'exercice de droits excessives ou manifestement infondées : article 12 ;
14) Pour l'obtention ou la divulgation d'information par le responsable de traitement : article 14, paragraphe 5, point c) ;
15) Pour la compilation des opinions politiques dans le cadre des activités électorales : *considérant 56,*
16) Pour le droit à l'effacement et le droit à l'oubli : *considérant 65* et article 17 ;
17) Pour la limitation du traitement des données au lieu de l'effacement : article 18 ;
18) Pour autoriser le profilage : *considérant 73* et article 22 ;
19) Pour les restrictions aux droits des personnes et obligations des responsables de traitement : *considérant 59* et article 23;
20) Pour déterminer les responsabilités respectives des responsables de traitement conjoints : article 26
21) Pour déterminer les exigences sur la validité juridique d'un acte liant le responsable de traitement au sous-traitant : *considérant 81* et articles 28 et 29 ;
22) Pour les exigences relatives aux instructions du responsable de traitement à son sous-traitant, y compris pour obliger le sous-traitant à conserver les données après la fin du contrat avec le responsable de traitement: *considérant 81* et article 28 ;
23) Pour la sécurité des traitements : article 32 ;
24) Pour prévoir des analyses d'impact dans le cadre de l'adoption d'une législation nationale : *considérant 93* et article 35 ;
25) Pour la procédure de consultation préalable de l'autorité de contrôle dans le cadre de l'adoption d'une nouvelle législation ou de la mise en place d'un nouveau traitement de données dans l'intérêt public : article 36 ;

26) Pour obliger à la désignation d'un délégué à la protection des données : article 37 ;
27) Pour l'obligation de secret professionnel du délégué à la protection des données : article 38 ;
28) Pour encourager les codes de conduite et la certification : articles 40 et 42 ;
29) Pour l'accréditation des organismes certificateurs : article 43 ;
30) Pour conclure des accords internationaux : *considérant 102* et article 46 ;
31) Pour des transferts de données dans l'intérêt public : *considérant 111*;
32) Pour certains transferts dérogatoires : article 49 ;
33) Pour limiter les transferts de données vers un pays tiers ou une organisation internationale en l'absence de décision d'adéquation à certaines catégories : *considérant 112*; article 49 ;
34) Pour la création des autorités de contrôle : *considérant 117*;
35) Pour prévoir la coopération entre les autorités de protection des données nationales s'il en existe plus d'une : *considérant 119,* article 51 ;
36) Pour les conditions générales de désignation des membres et du personnel des autorités de contrôle : *considérant 121*, articles 51, 52, 53, 54,;
37) Pour les pouvoirs des autorités de contrôle : considérant 129, article 58 ;
38) Pour les instances auxquelles les autorités de contrôle font rapport : article 59 ;
39) Pour confier des pouvoirs d'enquête aux autorités de contrôle des autres Etats membres effectuant des enquêtes sur son territoire dans le cadre d'opérations conjointes : article 62 ;
40) Pour la désignation de l'autorité de protection des données participant au CEPD lorsqu'il y en a plusieurs : *considérant 119* et article 68 ;
41) Pour les actions collectives et pour les exigences concernant les associations pouvant agir en représentation : *considérant 142,* article 80 ;
42) Pour la désignation de la juridiction compétente sur le territoire : *considérant 143* ; article 78 et 82 ;
43) Pour les régimes de responsabilité : *considérant 146*, article 82 ;
44) Pour les sanctions administratives des responsables de traitement publics : *considérants 150* et article 83 paragraphe 7 ;
45) Pour prévoir des sanctions lorsque le Règlement n'a pas harmonisé les sanctions, y compris pénales : *considérants149 et 151* et article 84 ;
46) Pour l'articulation des dérogations nationales en matière de liberté d'expression et de droit à l'information et les dérogations spécifiques : *considérant 153* ; article 85 ;
47) Pour l'accès aux documents publics et la réutilisation des données du secteur public : *considérant 154* et article 86 ;
48) Pour fixer les conditions spécifiques du traitement d'un numéro national d'identification : article 87 ;
49) Pour les traitements de données des salariés : *considérant 155* ; article 88 ;
50) Pour les traitements des données à des fins archivistiques dans l'intérêt public, statistiques, scientifiques, historiques, pour prévoir les garanties appropriées nécessaires et les dérogations : *considérant 156*, article 89 (et articles 14 et 17) ;
51) Pour la recherche scientifique : *considérant 157* ;
52) Pour les traitements de données à des fins archivistiques dans l'intérêt public : *considérant 158* ;
53) Pour les traitements de données à des fins statistiques : *considérant 162* ;
54) Pour les statistiques publiques : *considérant 163)* ;
55) Pour limiter les pouvoirs des autorités de contrôle pour respecter le secret professionnel : *considérant 164* et articles 13, paragraphe 5, point d) et 90 ;
56) Pour les traitements de données des églises et associations religieuses : *considérant 165.*

Source : SGAE

ANNEXE N° 2 : RÉSOLUTION EUROPÉENNE ADOPTÉE PAR L'ASSEMBLÉE NATIONALE LE 23 MARS 2012 SUR LA PROPOSITION DE RÈGLEMENT RELATIF À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL ET À LA LIBRE CIRCULATION DE CES DONNÉES [(1)]

Article unique

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu l'article 151-5 du Règlement de l'Assemblée nationale,

Vu le traité sur le fonctionnement de l'Union européenne, notamment son article 16,

Vu la charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8,

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Vu la communication de la Commission européenne, du 4 novembre 2010, au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée : « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » (COM [2010] 609 final),

Vu la proposition de règlement du Parlement européen et du Conseil, du 27 janvier 2012, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des marchés) (COM [2012] 11 final/ n° E 7055),

1. Réaffirme son engagement en faveur d'une protection renforcée de la vie privée des citoyens. Cela constitue une exigence démocratique face à l'apparition de nouvelles technologies et à l'émergence d'acteurs mondiaux dont le modèle économique repose notamment sur le traitement commercial de données personnelles ;

2. Soutient les objectifs annoncés par la Commission européenne dans sa communication du 4 novembre 2010 précitée concernant la révision du

(1) XIIIe législature. Session 2011-2012. TA n° 888

cadre juridique européen en matière de protection de la vie privée et des données personnelles ;

3. Estime que la modernisation, l'harmonisation et la simplification des règles applicables favoriseront une meilleure prise en compte, par l'ensemble des acteurs, des exigences européennes sur ces questions, grâce notamment à une plus grande responsabilisation des responsables de traitement, qui devront prendre toutes les mesures nécessaires à la protection des données personnelles traitées ;

4. Se félicite à ce titre de l'introduction, au niveau européen, de nouvelles dispositions qui participeront à une meilleure protection des droits des citoyens ;

5. Rappelle les orientations figurant dans la déclaration parlementaire franco-allemande de la mission d'information de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique et de la commission d'enquête du Bundestag sur internet et la société numérique, en date du 19 janvier 2011 ;

6. Souligne ainsi l'inscription dans le texte proposé par la Commission européenne d'un droit à l'oubli pour les citoyens, qui devrait, dans un souci de réalisme, être applicable aux réseaux sociaux et qui permettra aux personnes d'obtenir plus simplement la suppression de leurs données personnelles par les responsables de traitement. Il conviendra toutefois de s'assurer que ce droit permette aux personnes concernées d'obtenir la suppression des données mises en ligne par un tiers ;

7. Se prononce également en faveur de l'introduction d'un nouveau droit à la portabilité des données personnelles pour les citoyens, qui pourront désormais obtenir, à leur demande, restitution des données traitées, et notamment celles publiées sur les réseaux sociaux, dans un format électronique qui permette leur réutilisation sur d'autres supports ;

8. Défend la proposition de la Commission européenne visant à modifier considérablement les règles de recueil du consentement des citoyens au traitement de leurs données personnelles. Cette disposition sera beaucoup plus protectrice puisque l'expression du consentement nécessitera désormais une action positive du citoyen. Son silence ou son inaction ne pourront plus être assimilés à un consentement implicite ;

9. Soutient la désignation de délégués à la protection des données au sein des administrations publiques et des entreprises de plus de 250 salariés. Cette disposition, particulièrement attendue par certaines autorités de protection

européennes, participera assurément à une meilleure prise en compte des règles applicables dans ce domaine et à une plus grande sensibilisation des structures publiques et privées à ces questions. Toutefois, le caractère obligatoire de la désignation pourrait être contre-productif, une attention particulière devant être portée à la situation des salariés désignés délégués à la protection des données ;

10. Exprime son opposition claire à l'inscription, dans le texte proposé par la Commission européenne, du critère du principal établissement du responsable de traitement, qui serait porteur de conséquences politiques et économiques extrêmement dommageables pour notre pays et pour l'ensemble du territoire européen ;

11. Considère que cette solution éloignerait les Européens des autorités compétentes et qu'elle irait à l'encontre de la construction d'une Europe politique et concrète, proche des préoccupations de ses citoyens. Elle favoriserait également la pratique du « forum shopping », et l'établissement d'entreprises au sein des États membres dont les autorités de protection privilégient une approche plus souple. Elle réduirait également considérablement l'attractivité des territoires français et européens ;

12. Défend une solution alternative, fondée sur le maintien de la compétence d'une autorité de protection d'un État sur tout traitement de données ciblant spécifiquement la population de cet État, quel que soit l'État membre sur lequel est établi le responsable de traitement ;

13. Exprime ses plus vives inquiétudes quant au mécanisme de coopération proposé par la Commission européenne, qui ne garantirait pas une information suffisante des autorités de protection, notamment dans les cas de traitement de données particulièrement sensibles, comme les données génétiques, biométriques ou les données de santé, réduisant considérablement les contrôles *a priori* sur ces traitements à risque. Elle soutient l'introduction de nouvelles dispositions permettant une coopération renforcée entre les autorités de protection afin notamment de garantir un contrôle rigoureux des traitements de données à risque ;

14. Regrette la concentration de pouvoirs considérables entre les mains de la Commission européenne, aux dépens des autorités de protection, quant à l'élaboration des lignes directrices en matière de protection des données personnelles et à la définition des modalités d'application des nouvelles dispositions. Elle défend un rééquilibrage de ces compétences au profit des autorités de protection qui bénéficient de l'expertise technique indispensable à cette mission ;

15. Appelle à un meilleur encadrement des transferts internationaux de données, qui doivent nécessairement préserver les pouvoirs de contrôle et d'autorisation de ces échanges des autorités nationales de protection. L'auto-évaluation des conditions de transfert par les responsables de traitement eux-mêmes conduirait à une baisse considérable du niveau de protection des droits des citoyens ;

16. Invite le Gouvernement français à se saisir de cette question dans les plus brefs délais et à défendre une réforme plus respectueuse des droits de nos concitoyens, en accord avec la position défendue publiquement par la Commission nationale de l'informatique et des libertés ;

17. Appelle à l'adoption, par les États membres de l'Union européenne et les États tiers, d'une convention internationale pour la protection des personnes à l'égard du traitement des données personnelles, comme le soutient la résolution de Madrid, adoptée par la 31e conférence internationale des commissaires à la protection des données et de la vie privée.

À Paris, le 23 mars 2012.

Le Président,
Signé : BERNARD ACCOYER