N° 344

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 8 mars 2018

RAPPORT D´INFORMATION

FAIT

au nom de la commission des affaires européennes (1) sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la **protection** *des* **données personnelles** *(n° 296, 2017-2018),*

Par M. Simon SUTOUR,

Sénateur

(1) Cette commission est composée de : M. Jean Bizet, *président* ; MM. Philippe Bonnecarrère, André Gattolin, Mmes Véronique Guillotin, Fabienne Keller, M. Didier Marie, Mme Colette Mélot, MM. Pierre Ouzoulias, Cyril Pellevat, André Reichardt, Simon Sutour, *vice-présidents* ; M. Benoît Huré, Mme Gisèle Jourda, MM. Pierre Médevielle, Jean-François Rapin, *secrétaires* ; MM. Pascal Allizard, Jacques Bigot, Yannick Botrel, Pierre Cuypers, René Danesi, Mme Nicole Duranton, MM. Thierry Foucaud, Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Daniel Gremillet, Mme Pascale Gruny, Laurence Harribey, M. Claude Haut, Mmes Christine Herzog, Sophie Joissains, MM. Guy-Dominique Kennel, Claude Kern, Jean-Yves Leconte, Jean-Pierre Leleux, Mme Anne-Catherine Loisier, MM. Franck Menonville, Jean-Marie Mizzon, Georges Patient, Michel Raison, Claude Raynal, Mme Sylvie Robert.

SOMMAIRE

Pages

AVANT-PROPOS

Le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (dit « RGPDP ») définit un niveau cohérent et élevé de protection des personnes physiques et lève les obstacles aux flux de données à caractère personnel au sein de l'Union. Il harmonise à cet effet les règles de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données dont il entend assurer une application homogène.

D'application directe dans les États membres sans qu'il soit besoin de procéder à une transposition, le RGPDP constitue dorénavant le cadre général de la protection des données personnelles applicable aux opérateurs de l'Union européenne ou offrant des biens et services aux citoyens et résidents de l'Union. Il renvoie toutefois à des mesures d'application internes, comme la désignation de l'autorité nationale de contrôle compétente. Surtout, face à la grande inégalité des régimes de protection au sein de l'Union européenne et pour répondre à la sensibilité particulièrement forte en la matière de certains États comme la France, il autorise les États membres à maintenir ou à introduire des dispositions nationales pour préciser davantage l'application de ses règles et leur laisse des « *marges de manœuvre* » pour compléter les dispositions concernant le traitement de catégories particulières de données à caractère personnel, dénommées « *données sensibles* ». Par ailleurs, il n'exclut pas que des législations sectorielles nationales spécifiques, dans des domaines qui requièrent des dispositions plus détaillées, précisent les circonstances des situations particulières de traitement, y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est alors licite.

Le projet de loi relatif à la protection des données personnelles transpose la directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et précise les modalités d'application en France du RGPDP. Dans la mesure où celui-ci ouvre des marges de manœuvre, la commission des affaires européennes du Sénat a souhaité s'assurer qu'il n'alourdissait pas à l'excès les règles nationales. La sur-transposition des textes européens peut en effet nuire au bon fonctionnement du marché intérieur et pénaliser, ce faisant, les consommateurs. De nature à générer une surcharge administrative et des coûts supplémentaires pour les entreprises, elle est en outre susceptible de nuire à leur efficacité concurrentielle.

Cette problématique préoccupe la Commission européenne[1] tout comme le Gouvernement français[2]. Celui-ci s'est ainsi engagé à limiter le nombre de normes, notamment lors de la transposition du droit européen en droit interne[3], et entend examiner le droit en vigueur pour identifier et évaluer les sur-transpositions existantes. De son côté, la commission des affaires européennes du Sénat a entrepris en janvier 2018, conjointement avec la délégation aux entreprises, une démarche de recensement, auprès des entreprises, des sur-transpositions que celles-ci estiment pénalisantes pour l'exercice de leurs activités[4].

La Conférence des présidents a en outre confié à la commission des affaires européennes, le 21 février dernier, à titre expérimental, une mission de veille sur l'intégration des textes européens en droit interne afin notamment d'informer le Sénat sur d'éventuelles sur-transpositions. C'est dans cette optique que la commission des affaires européennes a examiné le projet de loi relatif à la protection des données personnelles et a formulé plusieurs observations.

[1] *Voir notamment la communication au Conseil COM 2010/543 du 8 octobre 2010* « Une réglementation intelligente au sein de l'Union européenne ».

[2] *Voir notamment l'étude du Conseil d'État* « Directives européennes : anticiper pour mieux transposer » *(2015).*

[3] *La circulaire du Premier ministre du 26 juillet 2017 pose notamment que* « toute mesure allant au-delà des exigences de la directive est en principe proscrite ».

[4] *Une plateforme de consultation a été mise en place, dans un premier temps, à l'occasion de l'examen du projet de loi pour un État au service d'une société de confiance qui sera très prochainement examiné par le Sénat. La présidente de la délégation aux entreprises et le président de la commission des affaires européennes ont présenté une communication sur les réponses reçues lors d'une réunion commune le 8 mars 2018.*

I. LE RGPDP : UN CADRE UNIFIÉ, COHÉRENT ET ÉLEVÉ DE PROTECTION DES DONNÉES PERSONNELLES

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental formalisé tant dans la Charte des droits fondamentaux de l'Union européenne que dans le traité sur le fonctionnement de l'Union européenne[1].

Une première étape essentielle a été franchie en 1995 avec l'adoption de la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2]. Cette directive a défini un ensemble de principes directeurs communs, mis en place un cadre visant à permettre le libre flux des données à caractère personnel entre les États membres et prévu la création d'organismes nationaux indépendants chargés de la protection de ces données sur le modèle de la Commission nationale de l'informatique et des libertés (CNIL). Outre la protection de la vie privée des personnes, qui a été étendue aux contenus échangés par le biais des communications électroniques par une directive de 2002[3], la directive de 1995 avait également pour préoccupation de donner plus de lisibilité aux entreprises dans le cadre de la libre circulation des marchandises, des personnes, des services et des capitaux.

Le RGPDP actualise cette directive. D'application directe dans les États membres, il renforce la protection des citoyens tout en améliorant la sécurité juridique des entreprises et marque une nouvelle étape dans l'intégration européenne en matière de protection de ces données.

A. UN PROCESSUS DE DISCUSSION ET D'ADOPTION LONG ET MALAISÉ

Dès 2009, la Commission européenne a constaté que le cadre défini en 1995 n'était pas en mesure de prendre en compte la rapidité des évolutions technologiques et la mondialisation des réseaux d'échanges d'informations qui ont considérablement accru le nombre des données à caractère personnel collectées, utilisées et transférées, et ce d'autant que les écarts de transposition de la directive entre les États membres sont particulièrement forts. Pour mieux faire face à la progression de ces flux, notamment *via* les réseaux sociaux, l'informatique en nuage (ou « *cloud*

---

[1] *Respectivement, art. 8, §1 et art. 16, § 1.*

[2] *Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, qui ne concerne pas les traitements de données effectués dans le champ de la sécurité publique, la défense ou la sûreté de l'État.*

[3] *Directive 2002/58/CE du 12 juillet 2002 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 »).*

computing ») et les moteurs de recherche qui ont augmenté d'autant la perte de contrôle des données à caractère personnel, elle a estimé qu'il convenait de réviser le cadre européen et de procéder à une harmonisation renforcée.

Après une première phase de consultation des parties prenantes en 2009, suivie d'une communication fin 2010[1] sur une « *approche globale de la protection des données à caractère personnel dans l'Union européenne* » puis de nouvelles consultations en 2011, sur la base de sa « *Stratégie visant à renforcer les règles de l'Union européenne en matière de protection des données* », la Commission a présenté, le 25 janvier 2012, un « *paquet européen de protection des données personnelles* ». Celui-ci comprenait une proposition de règlement général sur la protection des données personnelles et une proposition de directive spécifique pour les données traitées dans le cadre de la coopération policière et judiciaire en matière pénale, destinées à harmoniser les règles applicables sur le territoire de l'Union européenne et dans les relations entre les États membres et les pays tiers pour renforcer la protection des personnes physiques à l'égard du traitement de ces données.

La sensibilité de certaines données personnelles, notamment en matière de santé, les enjeux de souveraineté et les demandes de simplification des entreprises sont à l'origine de la longueur du processus de discussion et d'adoption du règlement.

Le Parlement européen a modifié la proposition de règlement et l'a adoptée en première lecture le 12 mars 2014. Les négociations se sont ensuite poursuivies entre les délégations de la Commission européenne, du Parlement européen et du Conseil de l'Union européenne et ont pris fin le 15 décembre 2015 et le texte a finalement été adopté par le Parlement européen après plus de quatre ans de travaux.

1. Les débats au Parlement européen : finalité des traitements et transferts des données

Les points les plus discutés au Parlement européen ont été :

– l'encadrement du transfert des données vers les pays tiers ;

– les sanctions pour les entreprises qui ne respectent pas les règles ;

– l'affirmation du principe de finalité des traitements et le principe, en corollaire, de l'« intérêt légitime » du responsable du traitement pour une autorisation autre de traitement des données personnelles ;

– le droit à l'effacement de ses données personnelles ;

– le consentement explicite de la personne au traitement de ses données personnelles ;

[1] *COM (2010) 609 final du 4 novembre 2010.*

– le droit de la personne concernée à une information dans un langage simple et clair ;

– l'encadrement du profilage ;

– la mise en place de délégués à la protection des données personnelles dans les institutions publiques et les grandes entreprises responsables de ces traitements ;

– le droit pour les personnes concernées d'introduire une plainte auprès des autorités de protection des données de leur choix ;

– l'établissement d'une autorité compétente (« guichet unique ») pour toutes les activités de traitement.

S'agissant de la proposition de directive, au-delà de la nécessité d'appliquer un niveau de protection élevé aux données pénales à caractère personnel, le Parlement a surtout insisté sur l'encadrement du transfert de ces données à des pays tiers et l'interdiction de les utiliser à d'autres fins que celles pour lesquelles elles ont été collectées. D'une manière générale, il a souhaité que les autorités répressives aient accès aux données des personnes reconnues coupables d'une infraction pénale pour des motifs raisonnables, les données des autres personnes n'étant susceptibles d'être traitées que pour la durée nécessaire à l'enquête ou à des fins ciblées et préventives.

L'articulation de la proposition de directive avec la directive « PNR européen » sur le registre européen des passagers alors en cours de discussion et finalement adoptée en avril 2016, a en outre contribué à ralentir son processus d'adoption.

2. L'invalidation du « *safe harbour* » américain : l'arrêt *Schrems* de la CJUE

Le processus d'examen a également été perturbé par la décision rendue par la Cour de justice de l'Union européenne le 6 octobre 2015, invalidant le « *safe harbour* » établi en 2000 par voie d'accord entre la Commission européenne et le département américain du commerce, « *pour faciliter le commerce et les relations d'affaires entre les États-Unis et l'Union européenne* », qui fournissait un cadre juridique à la circulation des données à caractère personnel en provenance de l'Union vers les États-Unis.

La Cour a en effet estimé que la Commission européenne n'était pas compétente pour assurer que la législation en vigueur aux États-Unis garantissaient « *un niveau de protection adéquat* » dès lors que les entreprises souscrivaient à un code de conduite après autoévaluation et autocertification de conformité, ce qui leur permettait, sans autre autorisation, de procéder au transfert de données personnelles de citoyens européens.

Dès lors, le Parlement européen a souhaité mieux encadrer les décisions des autorités nationales de contrôle sur le niveau de protection

adéquat dans les pays tiers en prévoyant des mécanismes d'évaluation régulière et en élargissant les possibilités de suspension des transferts de données.

B. LES OBSERVATIONS INITIALES DU SÉNAT : MAINTIEN DE DISPOSITIONS NATIONALES PROTECTRICES ET SAISINE DE L'AUTORITÉ DE CONTRÔLE NATIONALE

Sur le rapport de votre rapporteur[1], les commissions des lois et des affaires européennes du Sénat[2] ont formulé un certain nombre d'observations sur la proposition de règlement de la Commission européenne, reprises par le Sénat dans une résolution européenne adoptée le 6 mars 2012[3], à l'issue d'un débat en séance publique.

Dans le même temps, la commission des affaires européennes a adopté, sur proposition de votre rapporteur, une proposition de résolution portant avis motivé sur la méconnaissance du principe de subsidiarité par la proposition de règlement, que votre rapporteur a rapportée devant la commission des lois[4] et qui est devenue résolution du Sénat le 4 mars 2012[5].

Votre rapporteur a ensuite présenté, au nom de la commission des affaires européennes, une seconde proposition de résolution européenne sur la protection des données personnelles[6] portant cette fois sur la proposition de directive, devenue résolution du Sénat le 12 mars 2013[7].

Pour l'essentiel, ces résolutions mettaient l'accent sur la nécessité de conserver la possibilité d'adopter des mesures nationales plus protectrices, de prévoir la faculté pour les citoyens d'exercer leurs droits auprès de leur autorité nationale de contrôle et de mieux encadrer les conditions du transfert des données sensibles à des pays tiers.

1. Sur le RGPDP : la nécessité pour les États membres de pouvoir adopter des mesures nationales plus protectrices et pour les citoyens de saisir leur autorité nationale de contrôle

Approuvant l'objectif poursuivi par la Commission européenne d'une approche globale de la protection des données à caractère personnel reposant sur une harmonisation des règles applicables sur le territoire de l'Union européenne et dans les relations entre les États membres et les pays

---

[1] *Proposition de résolution n° 406 (2011-2012) de M. Simon Sutour, déposée au Sénat le 22 février 2012.*

[2] *Rapport n° 446 (2011-2012) au nom de la commission des lois et avis n° 457 (2011-2012) au nom de la commission des affaires européennes sur le RGPDP.*

[3] *Résolution n° 110 (2011-2012).*

[4] *Rapport n° 447 (2011-2012) au nom de la commission des affaires européennes.*

[5] *Résolution n° 105 (2011-2012).*

[6] *Proposition de résolution n° 343 (2012-2013).*

[7] *Résolution n° 108 (2012-2013).*

tiers, ainsi que l'introduction de nouveaux droits (droit à l'oubli, obligation de portabilité des données personnelles, consentement exprès, limitation du profilage, délégué à la protection des données dans les entreprises et encadrement des transferts internationaux de données), la résolution estimait toutefois que ces garanties devaient être renforcées, en particulier :

– les obligations pesant sur les moteurs de recherche, afin que le droit à l'oubli soit complété par l'obligation de prévoir l'effacement automatique des contenus indexés après un délai maximum et de permettre aux intéressés d'obtenir la désindexation de ceux qui leur portent préjudice ;

– le droit à l'effacement des données personnelles publiées par un tiers, dans le respect de la liberté d'expression ;

– l'obligation de désigner un délégué à la protection des données y compris par les entreprises dont la principale activité est le traitement de telles données, quelle que soit leur taille ;

– les pouvoirs d'investigation préalable des autorités nationales de contrôle.

Elle souhaitait par ailleurs que les États membres aient la possibilité d'adopter des dispositions nationales plus protectrices. L'avis motivé du Sénat soulignait à cet égard que, dans un domaine touchant directement aux droits des citoyens, il convenait de ne pas priver les États membres de la possibilité de maintenir transitoirement des dispositions nationales plus protectrices, de manière à ce que l'harmonisation européenne ne puisse aboutir à une diminution des garanties.

L'avis motivé contestait par ailleurs le renvoi, par la proposition de règlement, à des actes d'exécution pris par la Commission européenne, en particulier sur le droit à l'oubli numérique.

Enfin, la résolution et l'avis motivé demandaient la suppression du dispositif de « guichet unique » afin que le citoyen puisse saisir l'autorité de contrôle de son pays de résidence, plus proche de lui et auprès de laquelle il a l'habitude d'accomplir ses démarches, alors que les propositions de directive et règlement retenaient la compétence de l'autorité nationale de contrôle du principal établissement du responsable du traitement de ses données.

La Commission européenne a répondu à ces observations le 14 novembre 2011. Elle a notamment précisé que les actes d'exécution seraient strictement circonscrits aux mesures techniques, notamment en matière d'effacement des données. Elle a par ailleurs mis l'accent sur le rôle des autorités nationales de contrôle, le Comité de protection des données assurant un suivi pour « *une application correcte et uniforme du droit européen* ». Enfin, elle précisé que l'autorité nationale de contrôle demeurait « *l'interlocuteur privilégié des individus situés sur son territoire* » et que celle-ci serait partie prenante à toute enquête concernant une plainte dont l'origine

se situe sur son territoire. Autant de motifs pour lesquels elle a conclu que la proposition de règlement ne soulevait pas de problème de subsidiarité.

2. Sur la proposition de directive : la nécessité de pouvoir maintenir des garanties nationales de protection plus exigeantes et de préciser les conditions de transfert de données à des pays tiers

La résolution du Sénat considère qu'assurer la sécurité des citoyens européens, à travers la coopération judiciaire et policière, tout en maintenant un niveau élevé de protection de leurs droits fondamentaux, en particulier sur leurs données personnelles, est un objectif essentiel.

Le Sénat estime que si le renforcement de cette coopération doit être soutenu, il est là encore nécessaire de préserver les garanties prévues par le cadre juridique national qui permet un haut niveau de protection des données à caractère personnel, motif pour lequel elle demande que la directive soit d'harmonisation minimale.

Il appelle par ailleurs à la clarification du régime applicable à certains fichiers de police administrative et s'inquiète des conséquences de l'exclusion des fichiers européens de sécurité (Europol, Eurojust ou Frontex) du champ d'application de la directive.

La résolution procède également à un examen critique détaillé des règles d'utilisation des données sensibles dont elle estime qu'elles ne devraient pouvoir être utilisées que de manière restrictive et n'être conservées que pour le temps strictement nécessaire.

Elle estime en outre que le dispositif relatif au transfert de ces données à des pays tiers est insuffisant et déplore les dérogations qui seraient admises sans conditions précises de mise en œuvre.

En conclusion, le Sénat appelle à un renforcement du rôle des autorités de contrôle nationales, tant dans la procédure de collecte des données que dans la supervision des systèmes de traitement de ces données.

C. UN CADRE UNIFIÉ RENFORCÉ ET DES MARGES DE MANŒUVRE NATIONALES

Adopté le 27 avril 2016 et applicable à compter du 25 mai 2018, le RGPDP fournit un cadre unifié, cohérent et élevé de protection des données des personnes physiques résidant sur le territoire de l'Union, qui s'impose aux opérateurs de l'Union ou offrant des biens et services aux citoyens et résidents de l'Union.

1. Des droits individuels renforcés

Le règlement renforce les droits des personnes (droit d'accès, droit de rectification, droit à la limitation du traitement) et en facilite l'exercice en définissant l'expression du consentement libre et pleinement informé (avec des conditions particulières pour les enfants). Il encadre en outre strictement la possibilité pour les responsables de traitements de données personnelles de soumettre les données qu'ils ont recueillies à un « profilage » informatique.

Il ouvre par ailleurs de nouveaux droits aux personnes, en particulier :

– un « droit à la portabilité » des données, qui permet à une personne de récupérer, sous une forme facilement réutilisable, les données qu'elle a fournies ;

– un droit d'opposition à la réutilisation des données personnelles ;

– le droit à l'effacement des données ou « droit à l'oubli » ;

– la possibilité pour les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données d'introduire des actions collectives ;

– le droit à réparation du dommage matériel ou moral causé par une violation du règlement.

En cas de méconnaissance de ces droits, et comme l'avait souhaité le Sénat, les intéressés peuvent introduire une réclamation auprès de l'autorité nationale de contrôle de leur lieu de résidence habituelle, de leur lieu de travail ou du lieu où la violation a été commise. En cas de traitement transfrontalier, l'autorité de contrôle de l'établissement responsable du traitement est toutefois l'« autorité de contrôle chef de file ».

Sans préjudice de ce recours administratif, les personnes peuvent également introduire un recours juridictionnel, directement ou par l'intermédiaire d'une association agréée.

2. Une logique de responsabilisation des opérateurs

Au régime d'autorisation par les autorités nationales est substituée une responsabilité première du responsable du traitement de données à caractère personnel visant à fournir des biens et services aux résidents européens ou à les « cibler ». Il doit mettre en œuvre des mesures techniques et organisationnelles pour s'assurer, et être en mesure de démontrer, que le traitement des données est effectué en conformité avec les règles applicables en matière de collecte, de traitement, de conservation et de sécurité de ces données. Lorsque qu'il constate une violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés

de l'intéressé, le responsable du traitement doit la notifier à l'autorité de contrôle au plus tard dans les 72 heures et en informer l'intéressé.

Pour les traitements réguliers et de grande ampleur effectués par une autorité publique ou un organisme public, le responsable du traitement désigne en outre un délégué à la protection des données, chargé de l'informer et de le conseiller, de contrôler le respect du règlement et de coopérer avec l'autorité de contrôle dont il est le point de contact.

Certains types de traitements présentant un risque élevé pour les droits et libertés des personnes, ils doivent faire l'objet d'une analyse d'impact préalable. La liste de ces traitements est établie et publiée par les autorités nationales. Dès lors que cette analyse fait apparaître que le risque serait élevé si des mesures spécifiques n'étaient pas prises pour l'atténuer, le responsable du traitement doit consulter l'autorité de contrôle. Cette consultation préalable peut en outre être imposée par le législateur national si le traitement est effectué dans le cadre d'une mission d'intérêt public.

Ces obligations s'imposent aux responsables du traitement et à leurs sous-traitants dès lors qu'une personne résidant en Europe est directement visée par un traitement de données. Toutefois, afin de tenir compte de la charge induite par le suivi des traitements de données personnelles, les entreprises comptant moins de 250 salariés sont dispensées de respecter certaines obligations en la matière, en particulier la tenue du registre des activités de traitement, sauf si les traitements qu'elles effectuent portent sur des données sensibles.

3. Le renforcement des autorités nationales de contrôle

Les autorités nationales de contrôle sont chargées d'accompagner les acteurs privés pour une bonne application du règlement. Elles doivent mener des actions de prévention, notamment en favorisant l'élaboration de codes de conduite tenant compte des différents types de traitements et de la taille des acteurs. Elles peuvent agréer des organismes experts pour contrôler le respect de ces codes et disposent d'un pouvoir de certification en matière de protection des données. Une capacité de certification peut également être reconnue à des organismes de certification qu'elles agréent.

Les autorités nationales de contrôle effectuent en outre des contrôles *a posteriori*, assortis de la capacité d'infliger des sanctions significatives susceptibles d'atteindre 4 % du chiffre d'affaires annuel mondial de l'entreprise[1]. Les exigences en matière d'indépendance, de pouvoirs d'enquête et de capacité à prendre des mesures provisoires coercitives (injonction, limitation temporaire du traitement, suspension des flux de données…) sont également renforcées.

[1] *La loi pour une République numérique a d'ores et déjà relevé à ce niveau le plafond des sanctions pécuniaires que la CNIL peut infliger.*

Les décisions des autorités de contrôle peuvent faire l'objet d'un recours juridictionnel.

Le règlement définit par ailleurs avec précision les modalités de coopération et d'assistance mutuelle entre les autorités de contrôle et de réalisation d'opérations conjointes.

4. Un Comité européen des données pour faire converger les pratiques

Le règlement institue un comité européen des données, qui remplace l'actuel groupe de travail dit « G29 », organe de l'Union européenne indépendant, doté de la personnalité morale, réunissant les présidents des autorités nationales de contrôle ou leurs représentants, créé par les articles 29 et 30 de la directive de 1995.

Conseil de la Commission européenne en matière de protection des données personnelles, le Comité européen des données est chargé de favoriser la convergence des pratiques par la publication de lignes directrices, recommandations et bonnes pratiques. Il veille à la conformité des décisions des autorités nationales à l'égard des codes de conduite, des critères d'agrément des organismes de certification et autres normes types sur lesquels il formule un avis. Le comité suit l'exploitation des marges de manœuvre laissées aux États. Enfin, il arbitre les divergences d'appréciation entre les autorités nationales de contrôle.

Dans le cadre de la préparation de l'entrée en vigueur du règlement général, les deux commissions des lois et des affaires européennes du Sénat, ont procédé conjointement, le 24 novembre 2016, à l'audition de la présidente de la CNIL qui présidait alors le G29. Mme Isabelle Falque-Pierrotin a notamment souligné le rôle clé conféré au Comité européen et précisé que « *la gouvernance est désormais distribuée, c'est-à-dire donnant le premier rôle aux autorités nationales, mais également intégrée, c'est-à-dire obligeant à une coopération sur les sujet d'intérêt commun*. »[1].

5. Une exportation contrôlée des données assortie d'une application extraterritoriale des règles européennes

Le règlement s'applique à tout établissement ou sous-traitant établi dans l'Union européenne, que le traitement des données à caractère personnel ait lieu ou non sur le territoire de celle-ci, comme à tout établissement ou sous-traitant qui n'est pas établi dans l'Union européenne pour les activités de traitement de données à caractère personnel de personnes physiques résidant dans l'Union européenne, dès lors que ces activités de traitement sont liées à l'offre de services ou de biens à ces

[1] *Voir le compte rendu de la semaine du 21 novembre 2016.*

personnes, quand bien même aucun paiement ne serait exigé des intéressés, ou au suivi d'un comportement au sein de l'Union européenne.

Sauf si le traitement présente un caractère occasionnel, les données ne peuvent être transférées dans un pays tiers que si la Commission européenne a pris à son égard une décision d'adéquation du niveau de protection ou moyennant l'existence de garanties appropriées, et à la condition que la personne concernée dispose de droits opposables et de voies de recours effectives. Des mécanismes de coopération internationale devront être mis en place en la matière.

L'Europe s'efforce de porter ce débat sur la souveraineté mais les discussions avec les États-Unis autour du « bouclier » sont loin d'être abouties, en particulier après le rejet du TIPP. Il convient donc que l'Europe reste particulièrement vigilante en la matière.

6. De nombreuses marges d'intervention laissées aux législateurs nationaux

S'il entend lever les obstacles aux flux de données à caractère personnel au sein de l'Union et assurer une application cohérente et homogène des règles de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données, le règlement autorise toutefois les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application de ses règles.

Surtout, il leur laisse des « *marges de manœuvre* » pour maintenir ou introduire des conditions supplémentaires pour le traitement de catégories particulières de données à caractère personnel, dénommées « *données sensibles* » (comme les données génétiques, les données de santé ou les données biométriques).

Par ailleurs, il n'exclut pas que des législations sectorielles nationales spécifiques fixent, dans des domaines qui requièrent des dispositions plus précises, les circonstances des situations particulières de traitement, y compris en définissant de manière plus détaillée les conditions dans lesquelles le traitement de données à caractère personnel est licite.

Enfin, pour l'exercice de missions d'intérêt public ou relevant de l'autorité publique, le règlement reconnaît aux États membres la possibilité de limiter certains droits, comme le droit à l'oubli ou le droit à la portabilité des données, ou encore le droit à ne pas faire l'objet d'une décision individuelle automatisée, dès lors qu'il s'agit de mesures nécessaires et proportionnées au regard de l'objectif poursuivi (sécurité, défense nationale, prévention des infractions, etc).

D. UNE DIRECTIVE POUR RENFORCER LA PROTECTION DES TRAITEMENTS DE DONNÉES À DES FINS DE PRÉVENTION, DE DÉTECTION ET DE TRAITEMENT D'INFRACTIONS PÉNALES ET FACILITER LA COOPÉRATION ENTRE LES ÉTATS

La directive (UE) 2016/680 du 27 avril 2016 remplace la décision-cadre de 2008[1] dont le champ était limité aux échanges des données pénales entre États membres de l'Union européenne ou entre ces États et des États tiers, les traitements de fichiers nationaux demeurant soumis aux législations nationales. Elle constitue dès lors un progrès notable dans l'harmonisation des règles applicables.

Le recours à un texte spécifique, qui n'est pas d'application directe, s'explique non seulement par les difficultés juridiques et politiques tenant aux positions de certains États membres (en particulier le Royaume-Uni, l'Irlande et le Danemark) mais tient également à la spécificité de ces fichiers au regard de leur finalité et de la nature publique du responsable du traitement des données.

La directive permet de garantir en la matière un même niveau de protection pour les personnes dans l'ensemble de l'Union européenne et d'éviter que des divergences de réglementation n'entravent les échanges de données. Le traitement de ces données n'est ainsi licite que dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente pour les finalités qui justifient leur collecte. Sont concernés tous les fichiers de police et de justice utiles à la prévention, à la poursuite et à la répression des infractions pénales ainsi qu'à leur exécution, y compris la protection contre les menaces sur la sécurité publique, mais pas les fichiers de renseignement qui ne relèvent pas du droit de l'Union.

Les règles posées par la directive sont pour partie les mêmes que celles que fixe le RGPDP, en particulier les principes en matière de traitement que sont la licéité et la loyauté, l'existence de finalités déterminées, explicites et légitimes, le traitement de manière adéquate, pertinente, non excessive des données et dans des conditions garantissant leur exactitude, leur sécurité et leur conservation pendant une durée raisonnable[2].

Les personnes investies de l'autorité publique ou les organismes auxquels a été confié l'exercice de prérogatives de puissance publique ainsi que les responsables de traitement sont soumis à des obligations comparables à celles qui s'appliquent aux entreprises : exigence de protection des données dès la conception et par défaut, obligation de tenir un registre des activités de traitement, d'effectuer une analyse d'impact en cas de risque élevé pour les droits et libertés de la personne concernée, de

---

[1] *Décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.*
[2] *Art. 4.*

notifier à l'autorité de contrôle ou de communiquer à la personne les violations de données personnelles qui la concernent ou de désigner un délégué à la protection des données.

En raison de la nature particulière de ces traitements, la personne concernée ne bénéficie toutefois pas d'un droit d'opposition. Quant à ses droits d'accès, de rectification ou d'effacement ou encore à être informée (dès l'enregistrement des données ou en cas de violation de celles-ci), leur portée peut être réduite dès lors qu'une limitation entière ou partielle constitue une mesure nécessaire et proportionnée pour l'efficacité des enquêtes et des procédures, celle de la prévention ou de la détection d'infractions pénales, protège la sécurité publique, la sécurité nationale ou les droits et libertés d'autrui.

Des mesures techniques et organisationnelles doivent par ailleurs être mises en œuvre par le responsable du traitement ou le sous-traitant afin de garantir un niveau de sécurité adapté au risque, en particulier contre toute introduction frauduleuse dans le système ou toute lecture, copie, modification ou suppression non autorisées de données.

II. LE PROJET DE LOI : RÉVISION DE LA LOI FONDATRICE DE 1978, EXPLOITATION DE CERTAINES DES MARGES DE MANŒUVRE DU RGPDP ET TRANSPOSITION DE LA DIRECTIVE SUR LES TRAITEMENTS DE DONNÉES PÉNALES

Le projet de loi modifie pour l'essentiel la loi fondatrice du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin de la mettre en cohérence avec le RGPDP, qui se substitue dorénavant à nombre des dispositions de celle-ci, tout en maintenant des dispositions particulières à certaines catégories de données, et la directive (UE) 2016/680 sur les traitements en matière pénale. Le titre II regroupe les dispositions qui s'inscrivent dans les marges de manœuvre ouvertes par le règlement aux législateurs nationaux. Enfin le titre III modifie les dispositions relatives aux traitements de données à des fins de prévention, de détection et de traitement d'infractions pénales, conformément à la directive.

A. L'AMÉNAGEMENT ET LE RENFORCEMENT DES POUVOIRS ET DES COMPÉTENCES DE LA CNIL

Le projet de loi désigne la CNIL en qualité d'autorité nationale de contrôle chargée de veiller à l'application du règlement et de la directive. Il adapte ses pouvoirs et compétence en fonction de ce que prévoient les deux textes européens.

1. Le renforcement des pouvoirs de contrôle a posteriori

Les pouvoirs de contrôle des membres et agents de la CNIL dans l'exercice des missions que leur confie le règlement, leur droit d'accès à tous les locaux à usage professionnel ou non, à l'exclusion des parties affectées au domicile privé, sont modifiés conformément au RGPDP. Les garanties entourant ces contrôles sont maintenues et le texte introduit, conformément au règlement, les exceptions tirées du secret liant l'avocat à son client, du secret des sources journalistiques et du secret médical. Enfin, il autorise les agents de la CNIL à utiliser des identités d'emprunt sur les réseaux dans le cadre des contrôles qu'ils effectuent.

2. L'interlocuteur du citoyen en cas de réclamation transfrontière

La liberté laissée par le règlement aux législations nationales en matière d'organisation de la coopération entre les autorités de contrôle est très réduite.

L'article 5 du projet de loi précise, comme l'avait souhaité le Sénat, que la CNIL reste compétente pour recevoir une réclamation affectant par

ailleurs d'autres États membres même si elle n'est pas chef de file de la coopération. Il prévoit en outre que, lors de la mise en œuvre de la coopération organisée par les articles 60 à 67 du règlement, les agents européens missionnés par les autres autorités nationales doivent être habilités par le président de la CNIL s'ils participent à des contrôles sur le territoire français (ce qui les place sous l'autorité de la CNIL), et que les contrôles auxquels ils procèdent s'effectuent dans le cadre légal français. Le projet de loi précise également que ces agents n'interviennent pas dans la procédure de coopération concernant les fichiers de souveraineté qui ne relèvent pas du RGPDP.

3. L'élargissement de la faculté de prononcer des astreintes

Les dispositions de la loi de 1978 relatives aux mesures et sanctions susceptibles d'être prises, selon le cas, par le président ou la formation restreinte de la CNIL, sont réécrites pour permettre à l'autorité de contrôle de prendre les mesures correctrices prévues par le règlement et la directive et compléter celles déjà existantes.

En outre, dans la mesure où l'article 84 du règlement et l'article 57 de la directive permettent de prévoir des sanctions supplémentaires dès lors qu'elles sont proportionnées et dissuasives par rapport à l'objectif de mise en conformité aux obligations des responsables de traitement, le projet de loi permet à la CNIL d'assortir d'une astreinte l'injonction faite à un responsable de traitement de se mettre en conformité avec la loi ou le RGPDP, ou de satisfaire aux demandes présentées par une personne concernée en vue d'exercer ses droits. Il retient par ailleurs la faculté prévue par l'article 83.7 du règlement de prévoir des amendes administratives quand un traitement est mis en œuvre par l'État, dans la limite de 10 millions d'euros.

4. La faculté de retirer certaines décisions

Le projet de loi complète les pouvoirs de la CNIL en introduisant la possibilité, non prévue par le règlement, de retirer la décision d'approbation d'une règle d'entreprise contraignante lorsque la CNIL constate, sans visée répressive, que les conditions légales ne sont objectivement plus remplies.

Il prévoit également qu'en cas de manquement à ses obligations commis par un organisme de certification ou un organisme chargé de veiller au respect d'un code, de non-respect du RGPDP ou de la loi de 1978, la CNIL puisse lui retirer son agrément.

B. UNE EXPLOITATION MESURÉE DES « MARGES DE MANŒUVRE » OUVERTES PAR LE RGPDP

Ainsi que l'indique l'intitulé de son titre II, le projet de loi exploite certaines des quelque cinquante « *marges de manœuvre* » ouvertes par le RGPDP.

Le champ d'application de ces règles nationales est limité aux personnes résidant en France, y compris lorsque le responsable du traitement n'y est pas établi. Dans le souci de protéger la liberté d'expression, et conformément à l'article 85.2 du RGPDP, il est toutefois renvoyé au droit national du responsable du traitement, dès lors que celui-ci est établi dans l'Union européenne, lorsque le traitement est réalisé à des fins journalistiques, universitaires, artistiques ou littéraires.

1. Un régime particulier révisé d'utilisation du numéro national d'identification des personnes

Les formalités préalables actuelles d'autorisation par décret en Conseil d'État des traitements utilisant le numéro national d'identification des personnes physiques (NIR) sont supprimées et il résulte de l'article 9 du projet de loi, qui réécrit l'article 22 de la loi de 1978, qu'un décret en Conseil d'État, pris après avis motivé et publié de la CNIL, déterminera les catégories de responsables de traitement utilisant le numéro national d'identification des personnes physiques (NIR) et les finalités admissibles de ces traitements. Sont toutefois exemptés de ces règles les traitements qui ont pour seules finalités la statistique publique, la recherche scientifique ou historique, sous réserve d'un traitement cryptographique préalable, ou encore la mise à disposition de téléservices par l'administration.

2. Des régimes particuliers pour certaines données dont le traitement répond à des objectifs d'intérêt général

Le projet de loi définit des règles particulières pour encadrer les traitements mis en œuvre pour le compte de l'État intéressant la défense, la sûreté, la sécurité publique ou qui ont pour objet la prévention et la répression des infractions pénales (sans préjudice de la protection des droits des victimes), les traitements mis en œuvre pour le compte de l'État qui portent sur des données génétiques ou biométriques d'identification des personnes ainsi que certaines catégories particulières de traitements portant par exemple sur les condamnations pénales et mesures de sûreté ou encore des données de santé.

Comme l'article 23 du règlement en prévoit la possibilité, il écarte dans certains cas le droit de la personne à la communication d'une violation de ses données pour tenir compte d'objectifs d'intérêt général (sécurité,

défense, prévention et détection des infractions…), et ce dans les limites autorisées par le règlement, pour des traitements dont la liste sera fixée par décret en Conseil d'État, après avis de la CNIL.

3. Des règles plus protectrices pour certaines catégories de données

Le projet de loi complète les dispositions particulières plus protectrices qui s'appliquent à certaines catégories de données en reprenant les exceptions admises par le règlement européen, par exemple le traitement des données biométriques aux fins d'identifier une personne physique de manière unique et celui de données génétiques.

Ces règles particulières s'appliquent y compris pour les traitements ne relevant pas du droit de l'Union européenne.

4. Des règles adaptées pour les traitements à des fins archivistiques ou de recherches historiques

Comme l'autorise l'article 89 du règlement, l'article 36 de la loi de 1978 est complété par l'article 9 du projet de loi pour faciliter et encadrer les traitements de données à des fins archivistiques ou de recherches historiques. Les conditions et garanties appropriées seront précisées dans le code du patrimoine.

L'article 36 de la loi de 1978 est en outre complété par l'article 12 du projet de loi pour ouvrir une faculté dérogatoire d'écarter les droits des personnes concernées (droit d'accès, de rectification, de limitation du traitement, de portabilité et d'opposition) lorsque ces droits rendent impossibles ou entravent sérieusement la réalisation des finalités spécifiques de ces traitements et où de telles dérogations sont nécessaires pour atteindre ces finalités.

5. Un régime ad hoc pour les données de santé

Le projet de loi reprend la définition des données de santé figurant dans le règlement qui en élargit le champ à toutes 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, et qui révèlent des informations sur l'état de santé de cette personne.

Il comporte un dispositif général, au sein d'un chapitre IX, régissant les traitements portant sur l'ensemble des données de santé, qui présentent une finalité d'intérêt public (section I) et un dispositif spécifique couvrant le cas particulier des traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (section II).

Dans la logique du RGPDP, le projet de loi fait de la déclaration de conformité aux référentiels, aux méthodologies de référence et du respect des règlements types, le principe, et de l'autorisation préalable par la CNIL, l'exception. Dans le régime de l'exception, il prévoit, pour les traitements dont les finalités de recherche ne sont pas encore identifiées, la saisine de l'Institut national des données de santé (INDS) par la CNIL ou son auto-saisine pour évaluer l'intérêt public du traitement. S'il maintient le délai de deux mois dans lequel la CNIL doit se prononcer, il en modifie la portée puisque l'absence de décision vaudrait désormais accord implicite, ce qui constitue une avancée pour les acteurs économiques.

La CNIL établira en la matière, en concertation avec l'INDS et des représentants des professionnels, des référentiels et des règlements-types pour faciliter la tâche des professionnels de santé. En particulier, elle précisera les modalités de recueil du consentement des personnes qui constitue l'un des éléments clés du RGPDP.

6. La possibilité pour l'administration de recourir à des décisions individuelles automatisées

Afin d'adapter les droits des personnes à un environnement administratif dématérialisé et ainsi que l'autorise l'article 22 du règlement, l'article 14 du projet de loi prévoit que l'article 10 de la loi de 1978 autorise l'administration à recourir plus largement à des décisions automatisées en fonction d'un algorithme, dès lors qu'elle offre des garanties aux administrés en matière d'information, de droits de recours et de maîtrise par le responsable du traitement.

C. UNE TRANSPOSITION ATTENTIVE DE LA DIRECTIVE

Le titre III du projet de loi procède à la transposition de la directive sur les traitements de données à caractère personnel en matière pénale.

Dans la mesure où les traitements mis en œuvre en France poursuivent souvent plusieurs objectifs, ce que ne prévoit pas la directive cet exercice n'a pas été aisé. A cet égard, les modalités de l'articulation avec les traitements aux fins de renseignement mériteraient d'être précisées.

L'article 19, qui introduit un chapitre XIII nouveau dans la loi de 1978, reprend l'ensemble des règles, y compris en matière de sécurité, prévues par la directive. Conformément à l'article 8.2 de celle-ci, il précise en outre les objectifs et les finalités de ces traitements, les données sur lesquelles ils peuvent porter et les autorités publiques ou organismes habilités à les mettre en œuvre. Si le traitement est mis en œuvre pour le compte de l'État, il doit, comme aujourd'hui, être autorisé par arrêté ou décret en Conseil d'État, après avis de la CNIL (article 70-3 nouveau de la loi de 1978).

Les articles 78-18 à 78-20 nouveaux de la loi de 1978 prévoient un exercice direct du droit d'accès et de rectification de la personne concernée, sauf s'il s'agit d'une décision judiciaire ou d'un dossier judicaire en cours de traitement (article 70-24), et sous réserve des restrictions autorisées par l'article 13.3 de la directive reprises aux articles 70-21 et 70-22 nouveaux de la loi de 1978. Par voie de conséquence, l'actuel exercice indirect des droits d'accès, de rectification et d'effacement de ces données, prévu à l'article 42 de la loi de 1978, est supprimé.

De la même manière, un droit à l'information de la personne concernée est introduit à l'article 32 de la loi de 1978, par l'article 18 du projet de loi, pour les traitements intéressant la police judiciaire.

III. LE MAINTIEN DE RÈGLES NATIONALES DE PROTECTION COMME SOUHAITÉ PAR LE SÉNAT SANS ALOURDIR LES CHARGES DES ENTREPRISES NI EMPÊCHER LA COOPÉRATION INTRA-EUROPÉENNE

Le projet de loi s'inscrit dans la logique de protection des données à caractère personnel du règlement et de la directive européenne et d'harmonisation de leur traitement, tout en mettant à profit certaines des marges de manœuvre qu'ils prévoient pour conserver des règles plus protectrices en matière de traitement des données sensibles, limiter les droits des personnes pour des motifs stricts de sécurité publique, confirmer l'allègement des obligations administratives des PME dont le traitement de données personnelles n'est pas l'activité essentielle.

En complément, l'Assemblée nationale a abaissé l'âge de consentement des enfants et introduit la possibilité de joindre une demande d'indemnisation dans le cadre d'un recours collectif.

Aucune de ces dispositions n'apparaît de nature à nuire aux droits des personnes, à entraver la circulation des données personnelles au sein du marché intérieur, dans les limites fixées par le RGPDP et la directive, ni à alourdir la compétitivité des entreprises françaises.

Quelques points particuliers méritent toutefois d'être signalés.

A. UNE MISE EN CONFORMITÉ À TRÈS BRÈVE ÉCHÉANCE : UN DÉFI POUR LES COLLECTIVITÉS TERRITORIALES

Le caractère tardif des mesures législatives d'application du RGPDP et la charge administrative, technique et financière généré soulèvent des difficultés pour les acteurs qui n'ont pu anticiper les obligations qui s'imposeront à eux dans quelques semaines, en particulier les petites collectivités territoriales qui ne disposent le plus souvent pas des moyens techniques et des financements nécessaires.

Si la mise en conformité a un coût budgétaire pour l'État et les collectivités territoriales, elle a également un coût économique non négligeable pour les entreprises. Toutefois, les PME employant moins de 250 salariés sont dispensées de la tenue d'un registre des données qu'elles traitent dès lors que le traitement de données à caractère personnel constitue pour elles une activité auxiliaire[1]. En outre, de manière générale, les entreprises n'ont pas l'obligation de procéder à la désignation d'un délégué à la protection des données lorsqu'elles n'effectuent pas de traitements à grande échelle ou de données sensibles[2]. Elles n'ont pas non plus l'obligation

[1] *Art. 30.5 du RGDPD.*
[2] *Art. 37 du RGPDP.*

d'effectuer une analyse d'impact pour les traitements qui ne sont pas susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques[1].

B. LE MAINTIEN DE RÈGLES NATIONALES PROTECTRICES POUR LES DONNÉES SENSIBLES

Dans la mesure où il exploite sans les excéder certaines des marges de manœuvre ouvertes par le règlement pour maintenir des régimes spéciaux pour les données les plus sensibles, il peut être considéré que le projet de loi ne procède pas *stricto sensu* à une sur-transposition de celui-ci.

Au surplus, ces dispositions s'inscrivent dans la logique du maintien d'un haut niveau national de protection en la matière souhaité par le Sénat dans les résolutions européennes qu'il a adoptées en 2012 et 2013, sans faire peser des charges supplémentaires sur les PME qui bénéficient des allègements autorisés par le RGPDP.

On observera toutefois que les conditions d'utilisation des traitements publics à des fins de Renseignement, qui ne sont pas traités en tant que tels par les textes européens et les droits afférents des personnes, mériteraient d'être précisés dans la loi.

C. LA QUESTION DE L'ÂGE DU CONSENTEMENT À LA COLLECTE, AU TRAITEMENT ET À L'UTILISATION DES DONNÉES PERSONNELLES

À l'Assemblée nationale, les échanges se sont concentrés pour l'essentiel sur l'âge du consentement, les algorithmes, les moteurs de recherche et la patrimonialisation des données, sans que ces derniers sujets aient emporté de modifications substantielles.

S'agissant de l'âge du consentement autonome des mineurs, le règlement le fixe à 16 ans mais prévoit que les États membres peuvent l'abaisser à 13 ans. L'Assemblée nationale a finalement fixé à 15 ans[2] l'âge en deçà duquel le consentement des parents est également requis. Il n'apparaît pas que cette approche mesurée, qui tient compte de la forte appétence des adolescents pour les échanges sur internet et de la nécessité d'une prise de conscience suffisante des risques associés à la communication incontrôlée de données à caractère personnel, puisse être contestée au regard du risque de su-transposition.

---

[1] *Art. 35 du RGPDP.*

[2] *Dans son rapport d'information n° 577 (15ème législature), la commission des affaires européennes de l'Assemblée avait proposé 13 ans, à la différence de la commission des lois qui préférait 15 ans.*

D. LE DROIT À RÉPARATION DANS LE CADRE DE L'ACTION DE GROUPE

Comme l'avait souhaité sa commission des affaires européennes, l'Assemblée nationale a introduit la possibilité d'obtenir, dans le cadre d'actions de groupe, non seulement la cessation du manquement aux obligations relatives à la protection des données personnelles[1], mais aussi des réparations pécuniaires.

Cette faculté n'est pas envisagée par le RGPDP, qui ne l'interdit toutefois pas. Elle est d'ailleurs prévue par le droit européen pour les autres actions de groupe, notamment en cas de manquement aux règles de concurrence.

Cette disposition ne constitue probablement pas une sur-transposition *stricto sensu* mais il serait préférable qu'elle soit introduite au niveau européen.

Par ailleurs, elle devrait probablement être un peu plus encadrée, en particulier par un renforcement des conditions d'enregistrement des associations autorisées à introduire des actions de groupe, auprès de l'autorité de contrôle nationale compétente en matière de protection des données à caractère personnel.

[1] *Cette faculté existe en droit français depuis la loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.*

EXAMEN EN COMMISSION

La commission des affaires européennes s'est réunie le jeudi 8 mars 2018 pour l'examen du présent rapport. À l'issue de la présentation faite par M. Jean-François Rapin, le débat suivant s'est engagé :

M. Jean Bizet, président. – Le sujet est complexe mais crucial. Les moyens de la CNIL, qui est présidée par une personne remarquable, doivent être renforcés pour pouvoir remplir les missions qui lui sont confiées. Quant à la mise en conformité des traitements de données des collectivités territoriales, le défi est d'importance pour elles.

Mme Sophie Joissains. – Je suis totalement en accord avec les observations proposées par Simon Sutour. La version finale du règlement comporte des avancées véritables qu'avait souhaitées le Sénat, en particulier la compétence de l'autorité de résidence. J'observe par ailleurs que le Gouvernement n'a pas abusé des marges de manœuvre ouvertes par le règlement.

La question des collectivités territoriales est cruciale. Seules 10 % d'entre elles sont en voie de mise en conformité. Ni le texte européen ni le projet de loi ne prévoient de marge de manœuvre en la matière. Or toutes les collectivités locales sont concernées, dès qu'elles ont une cantine scolaire qui tient compte des interdits alimentaires des enfants ou qu'elles enregistrent les skieurs qui font l'acquisition d'un forfait pour leur envoyer plus tard une publicité sur la station. On pourrait prévoir que la CNIL n'infligera pas d'amendes pendant deux ans, qu'elle accompagne en outre les collectivités territoriales, par exemple en déployant des points relais dans les territoires. La mutualisation des traitements doit également être encouragée.

Sur l'âge du consentement, nous avons entendu l'association e.Enfance qui préconise de le fixer à 13 ans dès lors qu'un régime spécifique de protection des enfants serait défini. La baisse éventuelle de l'âge du consentement pourrait être subordonnée à la mise en place de ce régime par les opérateurs qui doivent être responsabilisés en la matière. Le double consentement prévu par le règlement européen est purement déclaratif dans la mesure où il n'y a pas de procédure de vérification.

Je me félicite du regard de la commission des affaires européennes sur la transposition et de son souci de prévenir les sur-transpositions. Son rôle en amont, lors de la négociation, a été très actif. Les synergies permettent de renforcer notre influence.

M. André Gattolin. – Je remercie les rapporteurs. J'observe que le règlement fait une cinquantaine de renvois aux textes nationaux ce qui pourrait conduire à multiplier les régimes spécifiques. Or, il ne faut pas

perdre de vue les enjeux de compétitivité économique. On sait combien les petits États sont soucieux d'attirer la manne fiscale. Il faudrait donc voir à quel type de transposition ils ont procédé.

S'agissant de la CNIL, elle est dorénavant chargée d'un contrôle a posteriori mais il faut la doter de moyens suffisants. À titre de comparaison, il n'y a pas moins de 600 personnes au CSA, surtout des ingénieurs !

Les collectivités territoriales sont au cœur des cités intelligentes et il faut, pour les aider à s'adapter, trouver des solutions dans le peu de marge ouverte par le règlement. J'observe par ailleurs que sont dispensées des formalités les plus lourdes les entreprises employant moins de 250 salariés sauf si leurs activités de traitements de données sont importantes. Comment déterminera-t-on cette importance ? Aucune indication n'est fournie à cet égard ni par le règlement ni par le projet de loi. Enfin, je rappelle que l'action de groupe est très encadrée et qu'aujourd'hui deux associations seulement répondent aux critères.

Mme Laurence Harribey. – Dès le mois de décembre, je me suis inquiétée des conséquences du règlement pour les collectivités territoriales. La question écrite que j'ai adressée au Gouvernement est restée sans réponse à ce jour. Or, plus de la moitié de nos collectivités ont moins de 500 habitants et sont sollicitées par des cabinets qui leur proposent une mise en conformité moyennant un coût souvent trop élevé pour elles. Il me semble que les départements devraient avancer sur la mutualisation de leurs ressources en la matière. Par ailleurs, qui sera le correspondant pour les données personnelles ? Son niveau de compétence n'est pas précisé ni sa responsabilité juridique.

Mme Sophie Joissains. – La question de la responsabilité des collectivités territoriale est une question clé. Je vais proposer à la commission des lois de décaler de deux ans l'effectivité de celle-ci.

L'action de groupe me paraît devoir comprendre la réparation mais à condition que les associations qui les portent soient agréées comme c'est le cas en matière de consommation.

Le projet de loi a été rédigé très tardivement pour une entrée en vigueur au 25 mai 2018. Le texte, qui a souhaité conserver la loi de 1978 pour des raisons symboliques, est en l'état très peu lisible et se juxtapose au règlement général qu'il ne peut pas reproduire. Le Gouvernement renvoie à une ordonnance pour en clarifier la lecture, ce qui ne saurait susciter l'enthousiasme dans le contexte actuel.

À aucun moment, le projet de loi n'évoque les collectivités territoriales alors qu'il prévoit des dispositions spécifiques bienvenues pour les TPE/PME. Or, elles sont fortement impactées.

M. Jean Bizet, président. – La question de la valeur économique des données est soulevée par le droit à la portabilité. Quelle est votre position sur ce sujet ?

Mme Sophie Joissains. – Les conséquences d'une patrimonialisation des données sont trop graves pour que l'on puisse en accepter le principe. Le risque d'une cession à vil prix est en outre très fort.

M. André Gattolin. – Pierre Bellanger nous a récemment exposé dans le cadre de ses travaux sur la souveraineté numérique que les gens produisent des données sur autrui qui n'entrent pas dans la notion de données personnelles. Les intéressés ne peuvent donc pas les récupérer alors même qu'ils sont traçables sur un nombre croissant de réseaux sociaux.

M. Simon Sutour. – Il est effectivement intéressant de suivre le fil de son identité sur Google ! Je suis favorable à la réparation pécuniaire mais il faut l'encadrer.

M. Jean Bizet, président. – Nous allons envoyer ces observations à la commission des lois. Notre collègue Simon Sutour pourra d'ailleurs les appuyer devant elle puisqu'il en est membre.

*

À l'issue du débat, la commission des affaires européennes a, à l'unanimité, autorisé la publication du rapport d'information et adopté les observations dans la rédaction suivante :

OBSERVATIONS

① Le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (dit « RGPDP ») constitue un cadre général de protection des données personnelles au sein de l'Union européenne applicable également aux opérateurs installés hors de l'Union européenne qui offrent leurs biens et services aux Européens, destiné à lever les obstacles aux flux de données à caractère personnel au sein de l'Union et à assurer une application cohérente et homogène des règles de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données.

② Plus particulièrement,

③ – il renforce les droits des personnes (droit d'accès, droit de rectification, droit à la limitation du traitement) et en facilite l'exercice en définissant l'expression du consentement libre et pleinement informé, avec des conditions particulières pour les enfants ;

④ – il ouvre de nouveaux droits aux personnes, en particulier un « droit à la portabilité » des données, qui permet à une personne de récupérer, sous une forme facilement réutilisable, les données qu'elle a fournies, un droit d'opposition à la réutilisation des données personnelles et un droit à l'effacement des données ou « droit à l'oubli » ;

⑤ – il prévoit la faculté d'introduire des actions collectives en matière de protection des droits et libertés des personnes en matière de protection des données et un droit à réparation du dommage matériel ou moral causé par une violation des règles qu'il définit ;

⑥ – il supprime l'autorisation préalable des traitements de données à caractère personnel et prévoit que les responsables de ces traitements doivent mettre en œuvre des mesures techniques et organisationnelles pour s'assurer, et être en mesure de démontrer, que le traitement des données est effectué en conformité avec les règles applicables en matière de collecte, de traitement, de conservation et de sécurité de ces données ; il prévoit toutefois que les entreprises employant moins de 250 salariés peuvent être dispensées de certaines de ces obligations sauf si les traitements qu'elles effectuent portent sur certaines données sensibles et que les traitements présentant un risque élevé pour les droits et libertés des personnes doivent faire l'objet d'une analyse d'impact préalable ;

⑦ – il révise le rôle des autorités nationales de contrôle dont il conforte l'indépendance et les moyens, renforce les pouvoirs coercitifs et organise leur coopération en cas de traitements transfrontaliers ;

⑧ – il encadre l'exportation des données personnelles vers des pays tiers en la subordonnant à une décision d'adéquation du niveau de protection prononcée par la Commission européenne ou l'existence de garanties appropriées ;

⑨ – il laisse des « marges de manœuvre » aux États membres pour maintenir ou introduire des conditions supplémentaires pour le traitement des « données sensibles », n'exclut pas des législations sectorielles nationales spécifiques et reconnaît aux États membres, pour l'exercice de missions d'intérêt public ou relevant de l'autorité publique, la possibilité de limiter certains droits, dès lors qu'il s'agit de mesures nécessaires et proportionnées au regard de l'objectif poursuivi.

⑩ La directive UE 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales harmonise le droit européen en la matière en leur étendant les principes fixés par le RGPDP, sous réserve de restrictions justifiées par la nature des données et des finalités des traitements dont elles font l'objet.

⑪ Plus particulièrement,

⑫ – elle crée un droit à l'information de la personne dont les données sont traitées ;

⑬ – elle lui permet d'exercer directement les droits reconnus à la personne concernée (droit à l'information, droits d'accès, de rectification et d'effacement), sauf si restrictions justifiées par des motifs qu'elle encadre ;

⑭ – elle encadre les transferts de ces données vers des pays n'appartenant pas à l'Union européenne.

⑮ Vu l'article 2 de la déclaration des droits de l'Homme et du citoyen,

⑯ Vu le traité sur le fonctionnement de l'Union européenne, notamment l'article 16,

⑰ Vu la Charte sur les droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8,

⑱ Vu le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (dit « RGPDP »),

⑲ Vu la directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales,

⑳ Vu la résolution européenne du Sénat n° 105 (2011-2012),

㉑ Vu la résolution européenne du Sénat n° 110 (2011-2012),

㉒ Vu la résolution européenne du Sénat n° 108 (2012-2013),

㉓ Vu le projet de loi adopté par l'Assemblée nationale relatif à la protection des données personnelles,

㉔ La commission des affaires européennes fait les observations suivantes :

㉕ – elle constate que l'article 1er du projet de loi charge la CNIL d'accompagner les responsables de traitements de données à caractère personnel par la mise en place d'éléments de droit souple (lignes directrices, recommandations et référentiels) et prévoit, en matière de sécurité des données, qu'elle élabore des règlements types de sécurité et qu'elle peut procéder à une évaluation préalable des risques et certifier des organismes compétents en la matière, autant de mesures, prévues par le règlement, qui sont de nature à faciliter la tâche des entreprises et des administrations ;

㉖ – elle regrette toutefois le caractère tardif des mesures d'application du RGPDP, qui est susceptible de soulever des difficultés, en particulier pour les collectivités territoriales qui n'ont pas toujours pu anticiper les nouvelles obligations qui s'imposeront à elles dans quelques semaines, sans compter qu'elles représentent pour elles un coût non négligeable ;

㉗ – elle observe en revanche avec satisfaction que les entreprises employant moins de 250 salariés sont dispensées de certaines obligations administratives dès lors que le traitement de données à caractère personnel constitue pour elles une activité auxiliaire ;

㉘ – elle constate que le projet de loi maintient des régimes spéciaux et des règles nationales pour les données les plus sensibles, sans excéder les marges de manœuvre ouvertes par le règlement, dans le sens du maintien du haut niveau de protection nationale en la matière souhaité par le Sénat ;

㉙ – elle observe toutefois que certains traitement de données publics sont également utilisés à des fins de renseignement, mais que le projet de loi est peu explicite quant aux conditions d'une telle utilisation ;

㉚ – elle constate avec satisfaction que toute personne résidant en France peut saisir la CNIL en cas d'utilisation irrégulière de ses données personnelles, même si le responsable du traitement n'est pas établi en France, ce qui est de nature à assurer une effectivité et une proximité plus grande à la protection des droits des personnes physiques sur le territoire national ;

㉛ – elle insiste sur la nécessité impérative de s'assurer, tant au niveau national qu'au niveau européen, de la protection effective des données à caractère personnel et des droits des personnes en cas de transfert vers des pays tiers ;

(32) – elle relève que l'âge du consentement autonome des mineurs fixé à 16 ans par le règlement a été abaissé à 15 ans par l'Assemblée nationale ;

(33) – elle considère qu'il convient d'avoir une approche mesurée en la matière, qui tienne compte de la forte appétence des adolescents pour les échanges sur internet et de la nécessité qu'ils aient une conscience suffisante des risques associés à la communication et au traitement incontrôlés de leurs données personnelles ;

(34) – elle constate que l'Assemblée nationale a introduit la possibilité d'obtenir, dans le cadre d'actions de groupe exercées en France au nom de résidents français, non seulement la cessation du manquement aux obligations relatives à la protection des données personnelles, mais également des réparations pécuniaires ;

(35) – elle observe que cette faculté de demander une indemnisation n'est pas prévue par le règlement européen mais que celui-ci ne l'interdit pas ;

(36) – elle constate au surplus que cette faculté s'inscrit dans la logique d'autres actions de groupe prévues par le droit européen ;

(37) – elle estime toutefois qu'il serait préférable que cette faculté soit rapidement prévue et encadrée par un texte européen qui prévoirait également un renforcement des conditions d'enregistrement des associations autorisées à conduire des actions collectives en matière de protection des données personnelles auprès de l'autorité nationale de surveillance.