ASSEMBLÉE NATIONALE

XIV^e LÉGISLATURE

Communication

Mercredi 14 mai 2014
16 h 30

Commission des affaires européennes

Communication de M^me Marietta Karamanli sur le paquet législatif relatif à la protection des personnes physiques à l'égard du traitement des données personnelles (COM(2012) 11 final – E 7055 et COM(2012) 10 final – E 7054)

ASSEMBLÉE NATIONALE

COMMUNICATION SUR LE PAQUET LÉGISLATIF RELATIF À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES PERSONNELLES

de M^me^ Marietta Karamanli

Proposition de directive du Parlement européen et du Conseil 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
COM(2012) 10 final – E 7054

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 et à la libre circulation de ces données
COM(2012) 11 final – E 7055

Réunion de commission du 14 mai 2014

La protection des données à caractère personnel au sein de l'Union européenne relève actuellement, hormis pour les questions relevant de la politique européenne de sécurité et de défense et de la coopération policière et judiciaire pénale, de la directive 95/46/CE du 24 octobre 1995 (1).

Ce cadre juridique a été élaboré alors que l'utilisation d'internet n'en était qu'à ses débuts. Or, depuis l'entrée en vigueur de cette directive, les technologies mais également les comportements des utilisateurs ont considérablement évolué. Le développement des sites internet de réseaux sociaux en est probablement l'exemple le plus frappant, mais d'autres technologies posent également des questions complexes, telles que les outils de géolocalisation ou le *cloud computing*

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

(« informatique en nuage ») qui permet le stockage de grandes masses de données sur des serveurs lointains.

Avec l'entrée en vigueur du traité de Lisbonne, la protection des données personnelles a été consacrée comme un droit nouveau.

En effet, le traité donne force juridique contraignante à la charte européenne des droits fondamentaux, dont l'article 8 dispose que *« toute personne a droit à la protection des données à caractère personnel la concernant »*, et précise que 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* ». Une autorité de contrôle indépendante doit veiller au respect de ces règles.

L'article 16 du traité sur le fonctionnement de l'Union européenne consacre lui aussi ce droit, et prévoit qu'il appartient au Parlement européen et au Conseil, statuant conformément à la procédure législative ordinaire, d'adopter les règles relatives à la protection des personnes à l'égard du traitement de leurs données personnelles et à la libre circulation de leurs données.

C'est dans ce contexte que la Commission européenne a présenté deux textes le 25 janvier 2012 : une proposition de règlement général sur la protection des données et une proposition de directive spécifique aux données policières et judiciaires.

L'Assemblée nationale s'est prononcée sur ces deux projets de texte dès leur présentation par la Commission européenne :

- sur la proposition de règlement, par les rapports de MM. Patrick Bloche [(1)] et Philippe Gosselin [(2)] et l'adoption d'une résolution le 23 mars 2012 (cf. annexe 1) ;

- sur la proposition de directive, par une communication suivie de conclusions, présentées par M. Geoffroy le 14 février 2012 (cf. annexe 2).

Depuis janvier 2012, l'examen de ces textes au Conseil est apparu très laborieux, tant du fait de leur extrême complexité technique que de fortes réserves politiques de la part de certains États membres. Pour le moment, l'accent a surtout été mis sur la négociation de la proposition de règlement, et la négociation de la proposition de directive a peu avancé au Conseil.

---

(1) Rapport n° 4326 du 7 février 2012 de M. Patrick Bloche sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'Union européenne, notamment dans le cadre de la réforme de la directive 95/46/CE.

(2) Rapport n° 4325 du 7 février 2012 de M. Philippe Gosselin 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.

Les révélations d'Edward Snowden autour du programme « PRISM » ont donné un nouvel élan aux négociations. La Commission européenne a insisté sur la nécessité d'adopter le paquet législatif au printemps 2014. Plus en retrait, les chefs d'État et de gouvernement européens ont conclu lors du Conseil européen des 24 et 25 octobre 2013 à la nécessité de l'adoption de ce paquet législatif « *en temps voulu* » d'ici 2015.

Bien qu'un accord tarde à se dégager autour de ce paquet législatif, la question de la protection des données personnelles est donc revenue au centre de l'agenda européen au cours des derniers mois. C'est ce qu'a rappelé encore plus récemment la décision de la Cour de Justice de l'Union européenne invalidant la directive sur la rétention des données télécoms, qui permettait aux opérateurs de stocker entre six mois et vingt-quatre mois les données de téléphonie des utilisateurs, considérée par la Cour comme « *une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, sans que cette ingérence soit limitée au strict nécessaire* » (1).

Toutefois, la réflexion autour de la question de la protection des données personnelles ne peut pas et ne doit pas se limiter à un simple phénomène de réaction à l'actualité. Il s'agit désormais d'un droit fondamental à part entière, « *au croisement du droit de propriété – les données qu'une personne diffuse sur un réseau social lui appartiennent-elles encore ? – de la liberté d'expression – notamment via les blogs – et de la protection de la vie privée* », pour reprendre les mots de la présidente de la CNIL (2).

Une réflexion de fond et de long-terme doit donc impérativement être menée sur ces sujets complexes.

Dans la perspective du Conseil Justice et Affaires intérieures du 5 et 6 juin prochain, au cours duquel une approche générale partielle doit être adoptée sur le projet de règlement – *a minima* sur le chapitre V relatif aux transferts internationaux, votre rapporteure a souhaité, non pas présenter à nouveau ces textes de façon exhaustive, mais faire un point d'étape sur leur évolution, et notamment sur les amendements adoptés en session plénière au Parlement européen le 12 mars dernier.

I. SUR LA PROPOSITION DE RÈGLEMENT

A. LE TEXTE DE LA COMMISSION EUROPÉENNE

Le texte proposé par la Commission européenne est ambitieux.

---

(1) CJUE, 8 avril 2014, arrêt dans les affaires jointes C-293/12 et C-594/12 Digital Rights Ireland et Seitlinger.

(2) Isabelle Falque-Pierrotin, Nouveaux Cahiers du Conseil constitutionnel n° 36 (Dossier : La liberté d'expression et de communication), juin 2012.

Il l'est tout d'abord dans sa forme, puisque qu'il s'agit d'un règlement et non plus d'une directive, qui sera donc d'application directe et ne nécessitera pas de transposition, permettant ainsi une réelle harmonisation des droits nationaux.

Ce règlement est également ambitieux dans son contenu, puisqu'il vise à la fois à renforcer les droits des citoyens sur les données qui les concernent et à renforcer la sécurité juridique et pratique pour les responsables de traitement (entreprises et pouvoirs publics), nécessaire au développement de l'économie numérique.

Au-delà du renforcement des droits des personnes, le futur règlement doit répondre à un impératif : être technologiquement neutre, afin de s'adapter aux évolutions sans cesse plus rapides des technologies de l'information et de la communication.

Le règlement proposé par la Commission européenne prévoit ainsi de nouveaux droits pour les citoyens, en créant un *« droit à l'oubli numérique »* (article 17) et en garantissant un *« droit à la portabilité des données »* (article 18). Il consacre le principe du consentement explicite au traitement des données (article 7) et prévoit un meilleur encadrement de la pratique du profilage, c'est-à-dire du croisement de données personnelles pour obtenir un « profil » de la personne concernée (article 20).

La proposition de la Commission européenne étend également le champ d'application territorial des règles européennes de protection des données personnelles, puisque le règlement s'appliquerait non seulement au traitement des données à caractère personnel par des responsables de traitement établis dans l'Union européenne mais également au traitement des données personnelles par des responsables établis hors de l'Union européenne s'ils visent des résidents de l'Union européenne (article 3).

Par ailleurs, la proposition de la Commission européenne prévoit d'alléger les charges des entreprises, en supprimant l'obligation systématique de déclaration préalable à la mise en œuvre d'un traitement automatisé de données personnelles et en adoptant une approche fondée sur le risque : seuls les traitements susceptibles de présenter des risques particuliers pour les droits et libertés – déterminés par une analyse d'impact (article 33) – seraient soumis à une obligation de notification.

Parallèlement, les responsables de traitement seraient soumis à des exigences de sécurité accrues :

- les responsables de traitement devraient adopter des mesures qui répondent aux principes de la protection des données par défaut et dès la définition des moyens de traitement des données, dites de « *privacy by design* » (article 23) ;

- des « délégués à la protection des données » seraient obligatoirement désignés dans les entreprises de plus de 250 salariés et dans les organismes publics (article 35) ;

- des codes de conduite et des mécanismes de certification seraient mis en œuvre (article 38 et 39) ;

- la notification des failles de sécurité à l'autorité de contrôle et aux personnes concernées serait obligatoire (articles 31 et 32).

La proposition de règlement prévoit également des obligations propres aux sous-traitants (article 26), ce qui permettrait notamment de mieux prendre en compte la problématique de « l'informatique en nuage ».

Enfin, la proposition de règlement prévoit la création d'un Comité européen de la protection des données (CEPD), composé des directeurs des autorités de contrôle nationales et du contrôleur européen de la protection des données.

Un système de « guichet unique » serait mis en place afin de simplifier les démarches des entreprises : une seule autorité de contrôle serait compétente pour juger des éventuelles atteintes à la règlementation par un responsable de traitement si le responsable de traitement dispose d'établissements dans plusieurs États membres ou si le traitement concerne des citoyens résidant dans plusieurs États de l'Union européenne. L'article 51 de la proposition initiale de la Commission européenne prévoit que l'autorité de contrôle désignée comme le guichet unique soit celle de l'État où le responsable du traitement a son *« établissement principal »*.

B. LA POSITION DU PARLEMENT EUROPÉEN

Au Parlement européen, le rapport de Jan-Philipp Albrecht (Verts/ALE) a été adopté le 12 mars 2014 en plénière par 621 voix pour, 10 contre et 22 abstentions.

Ce rapport prévoit notamment d'augmenter le plafond des sanctions, qui pourraient désormais s'élever à 100 millions d'euros ou 5 % du chiffre d'affaires annuel mondial d'une entreprise lorsque celle-ci viole les règles européennes (contre 250 000 euros ou 2 % dans le texte de la Commission européenne) [(1)].

Sur la question du guichet unique, le Parlement européen propose la mise en œuvre d'une autorité chef de file [(2)], tout en maintenant le critère de l'établissement principal de traitement. L'autorité de contrôle chef de file ne prendrait des mesures qu'après consultation de toutes les autres autorités de contrôle concernées. Le Comité européen de la protection des données émettrait

(1) Article 79, amendement 188.

(2) Article 54 bis, amendement 168.

un avis sur l'identification de l'autorité chef de file en cas de difficultés. Si, au cours de l'examen de cas particuliers, des dissensions majeures émergeaient entre l'autorité chef de file et les autres autorités de contrôle, la question pourrait être examinée par le Comité européen de la protection des données, qui émettrait un avis dans un délai de six semaines.

Le Parlement européen a également fait le choix du renforcement de l'information des personnes, nécessaire à leur consentement éclairé : les amendements adoptés prévoient ainsi que les informations fournies doivent être « *claires et compréhensibles* », précisant notamment au moyen de textes et de pictogrammes quelles sont les données personnelles collectées ainsi que l'usage qui en est fait [(1)].

Le texte du Parlement européen réduit le nombre de cas dans lesquels le marketing direct [(2)] est considéré comme automatiquement licite, en les limitant aux produits et services du responsable de traitement initial ou au marketing par voie postale [(3)].

Il prévoit également un renforcement et une simplification du droit *d'opt-out* dans les cas licites de marketing direct, la personne concernée ayant le droit de s'opposer *« sans frais, à tout moment et sans autre justification au traitement de ses données personnelles »* [(4)].

Enfin, le Parlement européen répond en partie aux inquiétudes soulevées par les révélations autour du programme PRISM. Un nouvel article [(5)] a été introduit afin d'encadrer le transfert de données par des entreprises soumises au droit de l'Union européenne à des autorités publiques de pays tiers en faisant la requête. Lorsqu'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers demande à un responsable de traitement ou à un sous-traitant de divulguer des données à caractère personnel, celui-ci devrait obtenir l'autorisation de l'autorité européenne de contrôle compétente, créant ainsi un conflit de normes. L'entreprise devrait également informer les personnes concernées de cette demande.

Alors que la proposition de la Commission européenne prévoyait la création d'un nouveau droit, le droit à la portabilité des données, le Parlement européen a considéré que ce droit à la portabilité ne constituait pas un nouveau droit en tant que tel mais était simplement une « déclinaison » du droit d'accès aux données, et a donc intégré les mécanismes initialement prévu à l'article 18 au sein de l'article 15 relatif au droit d'accès.

---

(1) Article 10 bis, amendement 105 ; article 13 bis, amendement 109.

(2) Le marketing direct est une technique de communication et de vente consistant à s'adresser de manière personnalisée et individualisée aux potentiels clients ciblés.

(3) Considérant 39 ter, amendement 18.

(4) Article 19, amendement 114.

(5) Article 43 bis, amendement 140.

Le Parlement européen a en revanche consacré le droit de s'opposer au profilage, même si celui-ci n'est pas suivi d'effets juridiques. (1)

Le texte voté par le Parlement européen remplace le seuil des 250 salariés rendant obligatoire la désignation d'un délégué à la protection des données par un critère relatif au nombre de traitements effectués (plus de 5 000 personnes concernées sur une période de douze mois consécutifs).

Enfin, de nouvelles précisions ont été ajoutées concernant les données personnelles sensibles (2), ajoutant notamment *« l'orientation sexuelle ou l'identité de genre »* à la liste de ces données. Le Gouvernement français s'est montré défavorable à cet amendement, soulignant que des données relatives à l'identité sexuelle sont utilisées de manière très courante par l'administration française – et notamment par la sécurité sociale. Votre rapporteure considère que cette notion devrait être définie de manière plus précise.

C. CERTAINES QUESTIONS DOIVENT FAIRE L'OBJET D'UNE ATTENTION SOUTENUE

● Le guichet unique

La question du guichet unique est celle qui avait fait l'objet des plus vives critiques de la part de notre commission, qui avait souligné le risque que les entreprises cherchent à s'implanter dans des États membres réputés plus accommodants en la matière, ainsi que la complexité d'un tel système pour les citoyens européens.

L'avis du service juridique du Conseil du 19 décembre 2013 s'est inscrit dans le même sens.

Le service juridique du Conseil a en effet considéré que la proposition d'un guichet unique tel que conçu par la Commission européenne faisait prévaloir le fonctionnement du marché intérieur sur la protection des droits des citoyens, et n'était pas conforme à l'article 16 du traité sur le fonctionnent de l'Union européenne. Il a souligné la complexité du système ainsi conçu, et considéré que la nécessité pour les citoyens de former un recours contre un responsable de traitement auprès d'une autorité de contrôle d'un autre pays que le sien ne permettrait pas l'exercice d'un droit au recours effectif.

Les dernières discussions au Conseil ont permis de progresser sur la question du guichet unique : le dernier état du texte maintient le critère de l'établissement principal du responsable de traitement pour désigner l'autorité de contrôle chef de file, mais un mécanisme de coopération systématique entre celle-ci et les autorités de contrôle concernées serait mis en place.

---

(1) Article 20, amendement 115.

(2) Article 9, amendement 103.

L’autorité chef de file proposerait une mesure aux autres autorités de contrôle concernées qui pourraient s’y opposer, en motivant leur objection, dans un délai de quatre semaines. Dans ce cas, le dossier serait transféré au Comité européen pour la protection des données et ce dernier pourrait rendre un avis qui serait rendu public mais qui ne serait pas contraignant.

Le mécanisme de coopération entre les autorités de contrôle serait similaire en cas de plainte. Le dernier état du texte prévoit un mécanisme à double niveau selon la nature de la décision prise par les autorités de contrôle.

Ainsi, l’autorité de contrôle nationale saisie par un citoyen proposerait un projet à l’autorité chef de file, qui pourrait s’y opposer. En cas d’accord entre les autorités de contrôle pour le rejet de la plainte de la personne concernée, la décision serait prise par l’autorité saisie, ce qui permettrait à la personne concernée d’exercer un recours contre cette décision dans son propre État. A l’inverse, dans le cas où les autorités de contrôle décideraient de sanctionner le responsable de traitement, la décision serait prise par l’autorité chef de file.

Dans une déclaration du 16 avril 2014, le G29 (Groupe européen des autorités de protection des données) suggère un compromis entre la position du Parlement européen et les propositions actuellement à l'étude au sein du Conseil. Il insiste dans cette déclaration sur la nécessité que chaque autorité de protection au niveau national reste compétente sur son territoire pour appliquer le futur règlement, tout en appuyant l’idée d’un guichet unique pour les cas concernant des résidents de plusieurs pays de l’Union européenne. Enfin, le G29 insiste sur la nécessité pour l’autorité de contrôle désignée comme compétente de coopérer avec les autres autorités de contrôle concernées, ainsi que de donner davantage de compétences au Comité européen de protection des données en cas de désaccord.

Votre rapporteure est satisfaite de l’évolution des négociations sur ce sujet, qui répond en partie aux préoccupations qui avaient été exprimées par l’Assemblée nationale lors de l’examen de la proposition de règlement.

Cependant, pour que ce mécanisme soit véritablement efficace, l’avis du Comité européen de protection des données devrait être contraignant.

- **L’action de groupe**

Le droit au recours des personnes concernées pourrait être utilement renforcé par la possibilité de mettre en œuvre des mécanismes de recours collectif en cas de violation des règles de protection des données, permettant à des groupes de citoyens de combiner leurs différentes plaintes en un seul recours.

Pour le moment, l’article 73 de la proposition de règlement prévoit la possibilité pour tout organisme, organisation ou association œuvrant dans le domaine de la protection des données personnelles – cette possibilité a été ouverte à toute association « *agissant dans l’intérêt public* » par le Parlement européen – d’introduire une réclamation auprès d’une autorité de contrôle au nom d’une ou de

plusieurs personnes concernées ou de manière indépendante. Aucune possibilité de ce type n'est ouverte par le règlement en ce qui concerne les recours juridictionnels.

Dans un avis du 22 juin 2011, le contrôleur européen de la protection des données avait recommandé l'introduction dans la législation de l'Union européenne de mécanismes de recours collectif en cas de violation des règles en matière de protection des données, estimant que cette possibilité constituerait à la fois un moyen efficace de renforcer le droit au recours des personnes concernées mais également un moyen de dissuasion indirect pour les responsables de traitement.

Votre rapporteure considère que la mise en place d'une action de groupe en matière de protection des données aurait une forte portée symbolique mais aussi pratique, et doit donc être encouragée.

● **La notion « d'intérêt légitime »**

La notion « *d'intérêt légitime* » utilisée dans la proposition de règlement [(1)], et qui était déjà présente dans la directive 95/46/CE du 24 octobre 1995 [(2)] doit également faire l'objet d'une attention particulière. En effet, la proposition de règlement prévoit que le traitement de données personnelles soit licite à condition qu'une des situations suivantes s'applique :

- la personne concernée a consenti au traitement de ses données ;

- 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 de traitement est soumis ;

- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;

- le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ;

- le traitement est nécessaire *« aux fins des intérêts légitimes poursuivis par le responsable de traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée* ».

Il convient de garantir que cette notion très large ne soit pas utilisée de manière extensive afin d'écarter la nécessité du consentement explicite. Pour cela, il conviendrait de préciser les contours de cet *« intérêt légitime »*.

---

(1) Article 6) f).

(2) Article 7) f).

● **Sur la mise en œuvre du « droit à l'oubli »**

En ce qui concerne le « *droit à l'oubli* », renommé « *droit à l'effacement* » par le Parlement européen, aucune obligation de déréférencement à la charge des moteurs de recherche n'est pour le moment explicitement prévue par la proposition de règlement, ce qui risque de minimiser la portée de ce droit. Toutefois, la mise en place d'un véritable droit au déréférencement pourrait se heurter à des obstacles techniques importants ainsi qu'à la garantie de la liberté d'expression.

Votre rapporteure estime que d'autres pistes doivent également être étudiées, comme l'effacement par principe des données d'un profil d'utilisateur après un certain délai si aucun usage n'en est fait ou la possibilité pour les utilisateurs de définir une date de péremption de leurs publications, ou encore la possibilité pour les personnes concernées de s'adresser à l'hébergeur du site de publication afin d'obtenir la suppression de données personnelles en l'absence de réponse du responsable de traitement initial.

II. SUR LA PROPOSITION DE DIRECTIVE

A. LA PROPOSITION DE LA COMMISSION EUROPÉENNE

La présente proposition de directive vise à remplacer la décision cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

La principale évolution proposée par la proposition de directive consiste à étendre considérablement le champ d'application de la décision-cadre 2008/977/JAI. Elle ne s'appliquerait plus uniquement aux échanges de données entre États membres, mais également aux traitements de données effectués par les autorités compétentes au sein des États membres en matière de prévention et détection d'infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales (hors les activités ne relevant pas du champ du droit de l'Union et les traitements réalisés par les institutions, organes et organismes de l'Union).

La proposition de directive prévoit également de renforcer le droit des personnes concernées par le traitement de données personnelles.

Elle prévoit notamment un droit à l'information des personnes concernées (article 11). Cette information comprendrait notamment l'identité et les coordonnées du responsable du traitement et du délégué à la protection des données, les finalités du traitement, la durée pendant laquelle les données sont conservées, l'existence du droit d'accès, l'existence d'un droit de réclamation auprès de l'autorité de contrôle, les destinataires des données personnelles, y compris les pays tiers et les organisations internationales et toute autre information nécessaire au traitement loyal des données. Par ailleurs, des informations sur le

caractère obligatoire ou facultatif de la fourniture des données à caractère personnel seraient prévues.

Toutefois, les États membres pourraient, par la loi, retarder ou limiter la fourniture d'informations, compte tenu d'intérêts légitimes dans une société démocratique (éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, éviter de nuire à la poursuite d'infractions pénales, protection de la sécurité publique et de la sûreté de l'État, protection des droits et libertés d'autrui).

Un droit d'accès des citoyens aux informations les concernant est également prévu par l'article 12. L'article 14 prévoit que, notamment dans les cas où l'accès est limité, la personne devrait être informée de la possibilité de consulter les données de manière indirecte, par l'intermédiaire de l'autorité de contrôle.

Enfin, la proposition de directive prévoit un droit à la rectification et à l'effacement des traitements illicites, qui devrait s'exercer auprès du responsable de traitement.

Actuellement, en France, le droit à l'information ne s'applique pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales (1). Malgré les exceptions prévues par la proposition de directive, il s'agirait donc d'un renversement de la logique présidant au droit à l'information.

Ces changements majeurs ont été fortement critiqués par les personnes auditionnées par votre rapporteure, qui ont regretté que la proposition de directive prenne insuffisamment en compte les spécificités de la matière pénale.

Les transferts vers des pays tiers ne pourraient avoir lieu que s'ils sont nécessaires à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière, ou d'exécution de sanctions pénales (article 33).

Ces transferts seraient autorisés lorsque la Commission européenne a adopté une décision constatant le caractère adéquat du niveau de protection dans cet État tiers (ou dans un secteur de traitement de données dans cet État tiers ou une organisation internationale). En l'absence d'une telle décision d'adéquation, le transfert pourrait avoir lieu lorsqu'il existe des « *garanties appropriées* », qui devraient être offertes par un instrument juridiquement contraignant, tel qu'une convention internationale (articles 34 et 35).

En dehors des cas dans lesquels la Commission européenne a pris une décision d'adéquation et de ceux dans lesquels des garanties appropriées ont été établies, un transfert de données vers un pays tiers ou une organisation

---

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 32 paragraphe 6.

internationale pourrait également avoir lieu si le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne ou d'une autre personne, à la sauvegarde des intérêts légitimes de la personne dans les cas prévus par la législation nationale, si le transfert est essentiel pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un État tiers, s'il est nécessaire à des fins de prévention et de détection d'infractions pénales ou s'il est nécessaire à la constatation ou à l'exercice d'un droit en justice en rapport avec la prévention des infractions pénales.

B. LA POSITION DU PARLEMENT EUROPÉEN

Au Parlement européen, le rapport de Dimitrios Droustas (Verts/ALE) a été adopté le 12 mars 2014 en plénière avec une majorité nettement inférieure au rapport sur la proposition de règlement (371 voix pour, 276 contre et 30 abstentions).

Les propositions adoptées par le Parlement européen vont dans le sens d'un accroissement de la protection des droits des citoyens, en précisant notamment que la directive vise *« à renforcer, à clarifier, à garantir les droits des personnes concernées »*, qui devraient inclure *« la fourniture d'informations claires et facilement intelligibles sur le traitement des données, sur le droit d'accès, de rectification et d'effacement de ses données, le droit d'obtenir des données, le droit à un recours effectif ainsi que le droit à une indemnisation pour une opération illicite de traitement »* [(1)].

Des délais de conservation seraient mis en œuvre : les données traitées conformément à la directive devraient être supprimées par les autorités compétentes lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été traitées, et les autorités compétentes devraient mettre en place des mécanismes assurant la fixation de délais applicables à l'effacement des données à caractère personnel et un examen périodique de la nécessité de conserver ces données [(2)].

Les autorités compétentes ne pourraient traiter les données à caractère personnel que des seules catégories de personnes concernées (les personnes à l'égard desquelles il existe des motifs raisonnables de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale, les personnes reconnues coupables d'une infraction pénale, les victimes présumées d'une infraction pénale et les tiers à l'infraction pénale tels que les témoins). Les données de personnes autres que celles qui sont concernées ne pourraient être traitées que dans certaines conditions, par exemple si ce traitement est indispensable pour atteindre des objectifs ciblés et préventifs ou à des fins d'analyse criminelle [(3)].

---

(1) Article 9 bis, amendement 72.

(2) Article 4 ter, amendement 64.

(3) Article 5, amendement 65.

Les données génétiques ne pourraient être utilisées qu'afin d'établir un lien génétique dans le cadre de la fourniture de preuves, de la prévention d'une menace pour la sécurité publique ou de la commission d'une infraction pénale spécifique [(1)].

Enfin, les transferts internationaux de données seraient très fortement encadrés, puisque le texte du Parlement européen prévoit la possibilité pour la Commission européenne de prendre des décisions par lesquelles elle déclarerait qu'un pays tiers ou une organisation internationale n'assure pas ou plus un niveau de protection des données adéquat. Dans ce cas, le responsable du traitement ou le sous-traitant devrait offrir des garanties appropriées contenues dans un instrument juridiquement contraignant. De tels transferts devraient être autorisés préalablement par l'autorité nationale de contrôle.

C. LES DROITS DES PERSONNES CONCERNÉES DOIVENT ÊTRE RENFORCÉS, MAIS IL EST IMPÉRATIF DE PRENDRE EN COMPTE LES SPÉCIFICITÉS DE L'ACTION JUDICIAIRE ET POLICIÈRE

Votre rapporteure ne peut que se féliciter de la volonté de la Commission européenne et du Parlement européen de renforcer les droits des citoyens en matière de protection des données personnelles.

Toutefois, il est nécessaire de prendre en compte la spécificité de la matière pénale : c'est pour cette raison que les données policières et judiciaires font l'objet d'un instrument juridique spécifique, plus souple que le règlement.

Cette spécificité doit mieux être prise en compte dans le contenu du texte : le droit à l'information, le droit d'accès ou le droit de rectification ne sont pas forcément appropriés en tant que tels à des fichiers comme les fichiers de police ou de justice.

Le manque de pragmatisme de certaines propositions de la Commission européenne a également été souligné.

Ainsi l'obligation prévue à l'article 60 de la proposition de directive de réviser les accords internationaux conclus par les États membres afin d'assurer leur conformité à la directive dans un délai de cinq ans à partir de l'entrée en vigueur de celle-ci, si elle est entièrement légitime, semble irréalisable.

De même, la possibilité offerte à la Commission européenne par les amendements du Parlement européen d'adopter des décisions « négatives » par lesquelles elle déclarerait qu'un pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, ou même une organisation internationale n'assure pas un niveau de protection des données adéquat semble difficilement acceptable : outre des conséquences diplomatiques importantes, cette « liste noire » pourrait avoir pour effet d'obliger les États membres à dénoncer des accords existants avec

---

(1) Article 8 bis, amendement 70.

des pays tiers, sans avoir la possibilité de pouvoir les renégocier, et risquerait de mettre un frein à une coopération internationale nécessaire en matière de police et de justice.

*

* *

Sur ces deux projets de textes, un important recours à la comitologie (actes délégués et actes d'exécution) est prévu. Or, les questions techniques que soulève ce paquet législatif sont dans le même temps des questions éminemment politiques. Les textes adoptés par le Parlement européen et par le Conseil doivent donc impérativement contenir les dispositions essentielles, et le recours à la comitologie doit être limité aux questions mineures ou purement techniques.

*

* *

Enfin, votre rapporteure tient à souligner que la question de la protection des données personnelles est loin de se limiter à ces deux projets de texte.

Il convient notamment d'être très vigilant sur l'évolution des relations entre l'Union européenne et les États-Unis à ce sujet. Comme l'a souligné la résolution sur la surveillance de masse adopté par le Parlement européen le 12 mars dernier [(1)], la protection des données doit impérativement être exclue des négociations de l'accord de partenariat transatlantique de commerce et d'investissement. Une attention particulière doit également être accordée à la négociation de l'accord-cadre entre les États-Unis et l'Union européenne relatif au transfert de données et à leur traitement dans le cadre de la coopération policière et judiciaire [(2)].

Par ailleurs, la question de l'évolution du « *Safe Harbor* » (« sphère de sécurité ») doit être posée. Il s'agit un ensemble de principes de protection des données personnelles négocié entre les autorités américaines et la Commission européenne en 2001 : les entreprises établies aux États-Unis doivent adhérer à ces principes auprès du Département du Commerce américain afin d'être autorisées à recevoir des données en provenance de l'Union européenne. Dans sa communication du 27 novembre 2013 intitulée « Rétablir la confiance dans les

---

(1) Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

(2) Recommandation de la Commission au Conseil, d'autoriser l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, et les détecter ou de les poursuivre dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale du 26 mai 2010, COM(2010) 0252.

flux de données entre l'Union européenne et les États-Unis d'Amérique » [(1)], la Commission européenne a présenté 13 recommandations visant à améliorer le fonctionnement de cette « sphère de sécurité », et des solutions devraient être proposées afin de remédier à certaines déficiences de ce mécanisme avant l'été 2014. S'il est pour le moment préférable d'améliorer le « Safe Harbor » sans le renégocier, votre rapporteure considère que la question de sa renégociation devra toutefois être posée après l'adoption de la proposition de règlement.

Dans le même sens, il conviendra d'être attentif à l'évolution des négociations sur la modernisation de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »).

*

* *

Il est proposé à la Commission des affaires européennes *d'adopter les conclusions suivantes*, en l'état des informations dont elle dispose.

(1) Communication de la Commission au Parlement européen et au Conseil, Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique du 27 novembre 2013, COM(2013) 846.

CONCLUSIONS ADOPTÉES PAR LA COMMISSION
DES AFFAIRES EUROPÉENNES

Article unique

« La Commission des affaires européennes,

Vu l'article 8-4 de la Constitution,

Vu l'article 8 de la Charte européenne des droits fondamentaux,

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

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 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,

Vu la proposition de directive du Parlement européen et du Conseil 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 [COM(2012) 10 final, n° E 7054],

Vu la 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 et à la libre circulation de ces données [COM(2012) 11 final, n° E 7055],

Vu la résolution législative du Parlement européen du 12 mars 2014 sur la proposition de directive du Parlement européen et du Conseil 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,

Vu la résolution législative du Parlement européen du 12 mars 2014 sur la 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 et à la libre circulation de ces données,

1. Réaffirme son engagement en faveur de la protection des données à caractère personnel, qui est un droit fondamental à part entière pour les personnes concernées ;

2. Estime qu'il est primordial d'aboutir au plus tard en 2015 à une adoption simultanée de la proposition de règlement et de la proposition de directive précitées ;

3. Approuve la proposition du Parlement européen d'augmenter le plafond des sanctions à 100 millions d'euros ou 5 % du chiffre d'affaires annuel mondial d'une entreprise lorsque celle-ci viole les règles européennes en matière de protection des données à caractère personnel ;

4. Soutient l'introduction au sein de la proposition de règlement précitée d'un article prévoyant que lorsqu'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers demande à un responsable de traitement ou à un sous-traitant soumis au droit de l'Union européenne de divulguer des données à caractère personnel, celui-ci doit obtenir l'autorisation de l'autorité européenne de contrôle compétente ;

5. Se félicite des avancées obtenues depuis le début des négociations sur le mécanisme du guichet unique ;

6. Rappelle la nécessité d'aboutir à une solution qui n'éloigne pas les Européens des autorités compétentes et ne favorise pas l'établissement d'entreprises au sein des États membres dont les autorités de contrôle privilégient une approche plus souple ;

7. Souhaite que le Comité européen de protection des données soit doté de pouvoirs juridiquement contraignants en cas de désaccord entre l'autorité chef de file et les autres autorités nationales concernées ;

8. Demande la mise en œuvre d'actions de groupe en matière de protection des données à caractère personnel ;

9. Souligne la nécessité de préciser la notion « d'intérêt légitime » autorisant le traitement de données à caractère personnel sans que le consentement de la personne concernée soit requis ;

10. Est favorable à un encadrement plus strict du « *marketing direct* », en limitant le nombre de cas dans lesquels celui-ci est considéré comme automatiquement licite ainsi qu'en renforçant et simplifiant les mécanismes *« d'opt-out »* ;

11. Rappelle que la proposition de directive précitée doit permettre d'atteindre un juste équilibre entre la protection des données à caractère

personnel et la conduite des mesures de prévention des infractions, des enquêtes et des procédures pénales.

ANNEXE 1 : 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.

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 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.

ANNEXE 2 : CONCLUSIONS SUR LA PROPOSITION DE DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL RELATIVE À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES AUTORITÉS COMPÉTENTES À DES FINS DE PRÉVENTION ET DE DÉTECTION DES INFRACTIONS PÉNALES, D'ENQUÊTES ET DE POURSUITES EN LA MATIÈRE OU D'EXÉCUTION DE SANCTIONS PÉNALES, ET À LA LIBRE CIRCULATION DE CES DONNÉES

La Commission des affaires européennes,

Vu l'article 88-4 de la Constitution,

Vu l'article 8 de la Charte européenne des droits fondamentaux,

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

Vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,

Vu la 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 et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012) 11 final, n° E 7055],

Vu la proposition de directive du Parlement européen et du Conseil 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 [COM(2012) 10 final, n° E 7054],

1. Rappelle que le cadre européen de protection des données à caractère personnel doit permettre d'atteindre une réelle harmonisation des législations nationales à un niveau élevé de protection ainsi qu'un juste équilibre entre la protection des données personnelles et la conduite des mesures de prévention des infractions, des enquêtes et des procédures pénales ;

2. Soutient l'extension du champ d'application de la proposition de directive aux traitements de données effectués au niveau national dans les États membres ;

3. Juge que l'encadrement des transferts vers des États tiers ou des organisations internationales est incomplet, s'agissant notamment des possibilités de transferts moyennant des garanties appropriées, insuffisamment définies à ce stade. Il conviendra également de pallier l'absence de protections spécifiques pour le transfert des données issues d'un autre État membre ;

4. Estime que le dispositif de saisine d'une autorité de contrôle dans tout État membre, tel qu'il serait ouvert à toute personne concernée par le traitement de ses données personnelles, doit être précisé ;

5. S'interroge la pertinence de la clause de réexamen des accords internationaux antérieurs.