N° 343

SÉNAT

SESSION ORDINAIRE DE 2012-2013

Enregistré à la Présidence du Sénat le 7 février 2013

PROPOSITION DE RÉSOLUTION EUROPÉENNE

PRÉSENTÉE AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES [1]
EN APPLICATION DE L'ARTICLE 73 *QUATER* DU RÈGLEMENT

sur la **protection** *des* **données personnelles**,

PRÉSENTÉE

Par M. Simon SUTOUR,

Sénateur

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale.)

(1) Cette commission est composée de : M. Simon Sutour, *président* ; MM. Alain Bertrand, Michel Billout, Jean Bizet, Mme Bernadette Bourzai, M. Jean-Paul Emorine, Mme Fabienne Keller, M. Philippe Leroy, Mme Catherine Morin-Desailly, MM. Georges Patient, Roland Ries, *vice-présidents* ; MM. Christophe Béchu, André Gattolin, Richard Yung, *secrétaires* ; MM. Nicolas Alfonsi, Dominique Bailly, Pierre Bernard-Reymond, Éric Bocquet, Gérard César, Mme Karine Claireaux, MM. Robert del Picchia, Michel Delebarre, Yann Gaillard, Mme Joëlle Garriaud-Maylam, MM. Joël Guerriau, Jean-François Humbert, Mme Sophie Joissains, MM. Jean-René Lecerf, Jean-Louis Lorrain, Jean-Jacques Lozach, François Marc, Mme Colette Mélot, MM. Aymeri de Montesquiou, Bernard Piras, Alain Richard, Mme Catherine Tasca.

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

En mars 2012, le Sénat a adopté en séance publique une résolution sur la proposition de règlement général sur la protection des données. J'avais présenté la proposition de résolution au nom de la commission des lois dont j'étais le rapporteur, et de la commission des affaires européennes qui s'était saisie pour avis. Sur l'initiative de cette dernière, le Sénat avait aussi adopté un avis motivé au titre de la subsidiarité. Ce texte est encore loin d'être finalisé. Le Parlement européen devrait se prononcer en avril. La présidence irlandaise semble vouloir accélérer les réunions des groupes de travail du Conseil, en vue d'un accord – au moins partiel – d'ici juin.

Aujourd'hui, le Sénat se prononce sur une proposition de directive qui doit fixer le cadre de la protection des données dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale et qui se substituera à une décision-cadre de 2008.

I/ Quel est le contexte ?

La décision-cadre de 2008 s'applique au seul traitement des données à caractère personnel transmises ou mises à disposition entre les États membres (échanges transfrontières). Le traitement des données par la police et la justice dans le cadre d'affaires pénales au niveau national ne relève pas de cette décision-cadre. Cet instrument n'a donc pas permis d'harmoniser les niveaux de protection sur le territoire européen. En outre, les dispositifs existants (Système d'Information Schengen, Europol, traité de Prüm, etc.) n'ont pas été révisés. En conséquence, plusieurs régimes juridiques spécifiques coexistent au sein de l'Union européenne dans ce domaine.

Le contenu de la décision-cadre de 2008 avait par ailleurs été critiqué par les autorités de protection de données regroupées au sein du « groupe de l'article 29 » (ou G29) dont fait partie la CNIL. Parmi ces critiques, on peut relever en particulier l'insuffisant

encadrement des données dites « sensibles » et des transferts de données vers des États tiers ou encore le faible rôle dévolu aux autorités de protection.

La France disposait déjà d'un niveau de protection adéquat au sens de la décision-cadre, en particulier grâce à la loi « Informatique et Libertés », qui s'applique à tout traitement de données quelle que soit sa finalité. La décision-cadre n'a donc donné lieu à aucune mesure de transposition particulière en droit français.

Le traité de Lisbonne a par la suite établi le principe selon lequel toute personne physique a le droit à la protection des données personnelles la concernant (article 16 TFUE). Il a en outre créé une base juridique spécifique pour l'adoption de règles dans ce domaine, qui s'applique également à la coopération policière et à la coopération judiciaire en matière pénale.

II/ Quelles sont les difficultés posées par ce texte?

1/ La cohérence des dispositifs

Nous pouvons approuver le choix de la Commission européenne de traiter ces questions dans un texte spécifique. Les questions pénales sont profondément marquées par les traditions nationales et de grandes différences subsistent entre les États membres ; il apparaît donc difficile d'adopter un règlement.

Il faut aussi saluer le choix de prendre en compte tant les échanges de données entre États membres que les traitements des données à l'intérieur de chaque pays. C'est un progrès. Cela permettra une mise en cohérence et évitera les difficultés pratiques rencontrées dans la mise en œuvre de la décision-cadre de 2008 pour distinguer selon la destination des données.

En revanche, le champ d'application de la directive pose certains problèmes. On comprend mal l'exclusion des traitements mis en œuvre par les organismes européens (comme Europol, Eurojust ou Frontex, par exemple). Cela pose un problème de mise en cohérence et de lisibilité des dispositifs. En outre, il pourra être difficile de déterminer, pour certains traitements, s'ils relèvent de la directive ou du règlement général. De nombreux fichiers de police administrative, qui relèveraient, en l'état, de la proposition de règlement, devraient logiquement relever de la proposition de directive, afin de garantir une cohérence des règles applicables à ces fichiers « mixtes ». Ainsi, par exemple, le Fichier National des

Interdits de Stade (FNIS) est un fichier de police administrative, mais qui a pour finalité de préserver la sécurité publique.

2/ Le maintien du niveau de protection

Comme le Sénat l'a souligné lors de l'examen de la proposition de règlement, il convient de s'assurer que les garanties offertes par notre droit national ne seront pas réduites par la directive. Or, sur plusieurs aspects, le texte risque d'aboutir à un niveau moindre de protection.

Nous devons donc demander qu'une disposition expresse rappelle que la directive ne fournit qu'un seuil minimal de garanties et que les États membres peuvent prendre des mesures assurant un niveau supérieur de protection des données.

3/ Les délégations à la Commission européenne

Lors de l'examen de la proposition de règlement, nous nous étions opposés aux multiples délégations faites à la Commission européenne sur des sujets essentiels qui devaient relever du législateur européen. Pour les mêmes motifs, dans ce texte, nous ne pouvons accepter que la Commission puisse adopter des actes délégués pour préciser les critères et exigences applicables à l'établissement d'une violation des données.

4/ Le traitement des données

Le texte ne reprend pas le principe établi par la proposition de règlement selon lequel les données ne sont « traitées que si, et pour autant que, les finalités du traitement ne peuvent pas être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel ». De même, aucune disposition expresse ne limite l'accès aux données au personnel dûment autorisé des autorités compétentes qui en a besoin pour l'exécution de ses missions. Les obligations des responsables de traitement devraient aussi être davantage précisées au regard notamment des niveaux de sécurité qu'exigent ces traitements et des conditions exigées pour le transfert de données à caractère personnel vers des pays tiers à l'Union.

En outre, contrairement à la proposition de règlement, aucune disposition particulière n'est prévue en ce qui concerne le traitement de données relatives aux enfants. En matière pénale en particulier, des modalités de traitement spécifiques de telles données s'avèrent pourtant nécessaires.

Enfin, les rédactions retenues rendent, dans certains cas, peu effectives des garanties pourtant nécessaires. Par exemple, la directive prévoit que les distinctions entre les catégories de personnes concernées (mis en cause, témoin, victime, etc.) doivent être établies seulement « dans la mesure du possible ».

5/ L'utilisation des données sensibles

Lors de l'examen des projets PNR, le Sénat a toujours manifesté son opposition à l'utilisation de ces données. La loi « informatique et libertés » prévoit des conditions très strictes pour leur utilisation.

Or la condition prévue par la loi « Informatique et Libertés » (« dans la mesure où la finalité du traitement l'exige ») n'est pas reprise dans le texte, lequel définit de manière très large les exceptions au principe d'interdiction du traitement de ces données. Par exemple, les données sensibles pourraient être utilisées lorsque « le traitement est autorisé par une législation prévoyant des garanties appropriées ».

De même, les données biométriques, de plus en plus utilisées dans le cadre répressif, devraient faire l'objet d'un encadrement particulier, comme dans la proposition de règlement.

6/ La durée de conservation

Le texte se borne à préciser que les données ne doivent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées. Ce qui n'offre que de faibles garanties contre d'éventuels abus. Il ne prévoit aucun examen périodique de la nécessité de conserver des données traitées. Il faut être plus strict sur la durée de conservation.

7/ Les droits des personnes concernées

Dans ce domaine, il est nécessaire de prévoir des limitations. Mais, comme me l'a fait observer la CNIL, le texte doit clairement affirmer qu'il s'agit bien d'exceptions à un principe général, y compris en matière de « fichiers de police ».

Or le texte reste très évasif sur les droits des personnes. Par exemple, il prévoit que les responsables de traitement doivent « prendre toutes les mesures raisonnables » pour élaborer des règles transparentes et accessibles d'exercice des droits, contrairement à la proposition de règlement qui prévoit une obligation plus stricte.

L'absence de mention du droit d'opposition des personnes concernées est également problématique. Il existe des situations dans lesquelles les personnes, les victimes d'infraction en particulier, doivent être mises en mesure de s'opposer au traitement de leurs données à l'issue de la procédure judiciaire par exemple.

Enfin, les modalités concrètes d'exercice des droits des personnes concernées paraissent plus compliquées que dans la proposition de règlement, sans que ceci soit justifié par les finalités des fichiers de police et de justice.

8/ Les transferts de données à des pays tiers

Cet aspect est l'un des plus préoccupants de ce texte comme du règlement d'ailleurs. Les garanties ne sont pas suffisantes. En particulier, les responsables de traitement pourront évaluer eux-mêmes, en dehors de tout cadre juridique établi et de tout contrôle de l'autorité de protection des données, si le transfert est entouré de garanties appropriées.

En outre, des règles devraient être prévues pour les transferts ultérieurs de données transmises initialement par un État membre. Celui-ci devrait être consulté et donner son accord avant que ses données puissent être re-transférées à un autre État par le destinataire du premier transfert.

Enfin, le texte prévoit l'obligation pour les États membres de renégocier tous leurs accords internationaux dans un délai de 5 ans après l'entrée en vigueur de la directive. Cette obligation apparaît peu réaliste, qui plus est dans un délai aussi court.

9/ Le rôle des autorités de contrôle

Si le texte était adopté en l'état, le rôle et les pouvoirs de ces autorités seraient en retrait par rapport à la loi française mais aussi à ce qui est prévu dans la proposition de règlement.

Le pouvoir de contrôle *a priori* qui est exercé en France par la CNIL serait réduit : la consultation préalable des autorités ne serait requise que dans les cas où le traitement créé contient des données sensibles et lorsque le traitement utilise de nouvelles technologies susceptibles de porter atteinte aux droits fondamentaux. En outre, cette consultation n'aurait lieu que dans le cadre de la création d'un nouveau fichier et non pas pour ses modifications ultérieures.

Le pouvoir de contrôle *a posteriori* de la CNIL pourrait également être remis en cause : de nombreux pouvoirs prévus dans

le cadre du règlement ne sont même pas mentionnés, alors que la CNIL dispose, sauf exception, de pouvoirs similaires sur tous les traitements de données, quels que soient leur finalité ou le responsable du traitement.

Au total, il s'agirait donc pour la France d'un réel recul par rapport aux dispositions nationales en vigueur dont il faut absolument se prémunir.

Nous devons donc exprimer notre préoccupation sur tous ces points.

*

Pour ces raisons, votre commission des affaires européennes a conclu, à l'unanimité, au dépôt de la proposition de résolution qui suit :

PROPOSITION DE RÉSOLUTION EUROPÉENNE

① Le Sénat,

② Vu l'article 88-4 de la Constitution,

③ Vu l'article 2 de la Déclaration des droits de l'homme et du citoyen,

④ Vu le traité sur le fonctionnement de l'Union européenne, notamment son article 16,

⑤ Vu la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8,

⑥ Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,

⑦ 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 (texte E 7054),

⑧ Rappelle les principes qu'il a affirmés dans sa résolution du 6 mars 2012 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 (texte E 7055), en particulier sur la nécessaire compétence de l'autorité de contrôle du pays de résidence du citoyen dont les données à caractère personnel font l'objet d'un traitement, sur le renforcement indispensable du rôle de ces autorités de contrôle, sur le nombre excessif d'actes délégués et d'actes d'exécution qui relèveraient de la compétence de la Commission européenne, sur la possibilité qui devrait être laissée aux États membres de garantir un haut niveau de protection des droits des personnes concernées, et sur les dérogations

inopportunes aux obligations pesant sur les responsables de traitement en matière de transferts internationaux de données ;

⑨ Considère comme un objectif essentiel d'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 de leurs droits sur leurs données personnelles ;

⑩ Estime que l'efficacité de la coopération dans ce domaine sera renforcée par l'existence d'un ensemble de règles garantissant la transparence des traitements de données, la pertinence et la fiabilité des informations recueillies ou les conditions de réutilisation de ces données pour des traitements ultérieurs ;

⑪ Souligne la nécessité de préserver les garanties prévues par le cadre juridique national qui permet un haut niveau de protection des données personnelles et qui repose sur le principe fondamental selon lequel les traitements de données nécessaires dans le cadre des activités répressives de l'État doivent être mis en œuvre conformément aux principes généraux de protection des données, tout en bénéficiant des dérogations justifiées et adaptées à leurs besoins ;

⑫ Demande dès lors qu'une disposition expresse précise que la directive ne fournit qu'un seuil minimal de garanties et qu'elle ne prive pas les États membres de la possibilité d'adopter des dispositions nationales plus protectrices ;

⑬ Approuve le choix de rendre applicable le texte tant aux échanges de données entre États membres qu'aux traitements de données au niveau national ; estime que l'exclusion du champ d'application de la directive des traitements mis en œuvre par les organismes européens (comme Europol, Eurojust ou Frontex, par exemple) posera un problème de mise en cohérence et de lisibilité des dispositifs ; juge nécessaire de clarifier le régime applicable à certains fichiers de police administrative afin de garantir une cohérence des règles applicables à ces fichiers ;

⑭ Conteste que la Commission européenne soit habilitée à adopter des actes délégués pour préciser les critères et exigences applicables à l'établissement d'une violation des données, sans même consulter les autorités de contrôle ;

⑮ Considère que les données à caractère personnel ne devraient pouvoir être traitées que si, et pour autant que, les finalités du traitement ne peuvent pas être atteintes par le traitement

d'informations ne contenant pas de données à caractère personnel ; qu'en outre, l'accès aux données devrait être strictement limité au personnel dûment autorisé des autorités compétentes qui en a besoin pour l'exécution de ses missions ; que les obligations des responsables de traitement devraient être davantage précisées au regard notamment des niveaux de sécurité qu'exigent ces traitements ; que des dispositions spécifiques devraient être prévues pour le traitement de données relatives aux enfants ;

⑯ Souligne que l'utilisation de données sensibles doit en principe être interdite ; que des dérogations à cette règle ne doivent être admises que dans la mesure où la finalité du traitement l'exige et sous réserve qu'un contrôle strict soit prévu ; considère, en conséquence, que le texte définit de manière trop large les exceptions au principe d'interdiction du traitement de ces données, en particulier pour le cas où le traitement est autorisé par une législation prévoyant des garanties appropriées ; juge nécessaire que le traitement des données biométriques soit soumis à un encadrement spécifique ;

⑰ Estime que la disposition selon laquelle les données ne doivent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées n'offre pas les garanties suffisantes ; que le texte devrait demander aux États membres de prévoir un délai de conservation des données et exiger qu'un examen périodique permette d'évaluer la nécessité de les conserver, sous le contrôle des autorités de protection ;

⑱ Considère que, s'il peut être nécessaire de prévoir, dans ce domaine, des limitations à certains des droits des personnes concernées, le texte devrait mieux affirmer qu'il s'agit d'exceptions à ces droits qui doivent être par ailleurs suffisamment garantis ; qu'un droit d'opposition devrait être prévu, au moins pour certaines catégories de personnes, et notamment les victimes d'infraction, qui doivent être mises en mesure de s'opposer au traitement de leurs données à l'issue de la procédure judiciaire ; qu'il conviendrait d'améliorer les conditions concrètes d'exercice de ces droits, et notamment la mise en œuvre des droits d'accès et de rectification, trop restrictivement prévus ;

⑲ Juge insuffisant le dispositif relatif au transfert de données à des pays tiers ; relève, en particulier, que les responsables de traitement pourraient évaluer eux-mêmes, en dehors de tout cadre juridique établi et de tout contrôle d'une autorité de protection des données,

si le transfert est entouré de garanties appropriées ; déplore que le texte prévoie des dérogations supplémentaires, qui seraient autorisées pour des fins particulières mais sans conditions précises de mise en œuvre ; estime que des transferts ultérieurs de données ne devraient être possibles que sous réserve de l'accord de l'État qui les a transmises initialement ; juge, en outre, peu réaliste l'obligation qui serait faite aux États membres de renégocier tous leurs accords internationaux dans un délai de cinq ans après l'entrée en vigueur de la directive ;

⑳ Souligne que le rôle des autorités de contrôle devrait être sensiblement renforcé, tant dans la procédure de collecte des données que dans la supervision des systèmes de traitement de données.