N° 108

S É N A T

Le 12 mars 2013

SESSION ORDINAIRE DE 2012-2013

RÉSOLUTION EUROPÉENNE

sur la **protection** *des* **données personnelles**.

Est devenue résolution du Sénat, conformément à l'article 73 quinquies*, alinéas 4 et 5, du Règlement du Sénat, la résolution adoptée par la commission des lois dont la teneur suit :*

Voir les numéros :

Sénat : **343** (2012-2013).

Le Sénat,

Vu l'article 88-4 de la Constitution,

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

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 loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

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),

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 ;

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 à 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 ;

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.

Devenue résolution du Sénat le 12 mars 2013.

Le Président,

Signé : Jean-Pierre BEL