



N° 4227

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 27 janvier 2012.

PROPOSITION DE 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,*

(Renvoyée à la commission des affaires européennes.)

présentée par

M. Philippe GOSSELIN,
député.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

La protection de la vie privée et des données personnelles de nos concitoyens représente, depuis de longues années, un enjeu majeur de politique publique dans notre pays. L'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et la création de la Commission nationale de l'informatique et des libertés (CNIL), ont fait de la France l'un des premiers pays au monde à se doter d'une législation et d'une autorité de contrôle indépendante sur ces questions.

Fort de son expérience dans ce domaine, notre pays a toujours été l'un des États les plus impliqués sur ces thématiques, aussi bien au sein de l'Union européenne que sur la scène internationale. Les principes de la loi du 6 janvier 1978 ont, pour une grande part, fortement inspiré les dispositions de la directive européenne 95/46/CE 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, dont l'adoption, en 1995, a constitué l'acte fondateur de la politique européenne dans ce domaine.

L'explosion d'Internet, l'émergence des réseaux sociaux, l'apparition de nouvelles technologies et de nouvelles pratiques ont considérablement transformé le monde numérique. Les données personnelles des citoyens ne sont plus seulement contenues dans des fichiers mis en place par les États ou les administrations, mais sont désormais traitées par différents acteurs publics et privés.

À cette nouvelle réalité s'ajoute l'internationalisation des échanges de données : les traitements de données sont désormais mondialisés et s'affranchissent des frontières traditionnelles, sans que les citoyens en soient nécessairement informés, et sans qu'ils puissent véritablement en conserver la maîtrise. Le recours, de plus en plus fréquent, au *cloud computing* et au stockage de données personnelles « en ligne » pose également de nouvelles questions à cet égard...

C'est dans ce contexte en forte évolution que la Commission européenne a fait de la révision de ce cadre juridique une priorité stratégique de son action, avec pour objectif premier l'harmonisation et la simplification des règles applicables en Europe.

Elle a ainsi lancé, dès 2009, une consultation publique de l'ensemble des acteurs du secteur, a publié, le 4 novembre 2010, la communication COM(2010) 609 final, intitulée « *Une approche globale de la protection des données à caractère personnel dans l'Union européenne* », et a très récemment, le 25 janvier 2012, proposé un Règlement pour l'ensemble des champs relevant de l'actuelle directive européenne de 1995, les questions relevant de l'ex-3^e pilier communautaire relatif au secteur police-justice faisant l'objet d'une directive.

L'Union européenne est donc à un moment charnière de sa politique de protection de la vie privée des Européens, et doit ainsi montrer toute sa capacité à moderniser le cadre juridique communautaire, tout en préservant sa tradition d'un haut niveau de protection des droits des citoyens européens.

Cette révision est porteuse de nombreuses avancées, attendues et nécessaires. Ainsi, les citoyens se verront reconnaître un droit à l'oubli numérique, les règles de recueil de leur consentement seront renforcées, les correspondants informatiques et libertés seront rendus obligatoires dans les administrations publiques et certaines entreprises ; ces dernières devront intégrer dans leurs politiques une démarche de protection des données personnelles (notion d'accountability) ; les sanctions contre les entreprises ne respectant pas les règles dans ce domaine seront considérablement renforcées... Toutes ces dispositions nouvelles, qui participeront à une meilleure transparence et à une information renforcée des citoyens quant aux traitements de leurs données personnelles, sont à saluer et favoriseront une meilleure protection des droits des citoyens.

Toutefois, certaines dispositions de ce projet de révision soulèvent des difficultés et suscitent l'inquiétude de plusieurs autorités européennes de protection, dont la CNIL.

En premier lieu, l'introduction du critère de l'établissement principal du responsable de traitement pour déterminer l'autorité compétente aura des conséquences politiques et économiques considérables.

Ainsi, pour un responsable de traitement installé dans plusieurs États membres de l'Union européenne, seule l'autorité de protection du pays accueillant le principal établissement de ce responsable sera compétente pour l'ensemble des traitements mis en œuvre sur le territoire communautaire. Par exemple, pour un traitement réalisé en France concernant des clients français, la CNIL ne sera pas nécessairement compétente pour traiter les plaintes de ceux-ci : sera compétente l'autorité

du pays dans lequel est installé le principal établissement de ce responsable de traitement.

Cette solution aura des conséquences politiques importantes, puisqu'elle participera à un éloignement sensible des citoyens des autorités compétentes. Comment les citoyens français pourront-ils en effet comprendre, et accepter, qu'une entreprise installée sur le territoire français, traitant des données personnelles de citoyens français, ne soit pas responsable devant la CNIL, mais devant l'autorité irlandaise, grecque ou suédoise ? Cette disposition ira ainsi à l'encontre de l'objectif de construction d'une Europe politique, transparente, de proximité, au fonctionnement compréhensible par tous. Elle renforcera au contraire l'image technocratique des institutions communautaires, allant à l'encontre de tous les efforts menés pour les rapprocher des citoyens européens. L'objectif doit être celui de la mise en œuvre d'un mécanisme intelligible, permettant à chaque citoyen désireux de défendre ses droits de pouvoir le faire rapidement et facilement auprès de l'autorité de protection de son État membre.

De plus, cette image technocratique sera également renforcée par le mécanisme de coopération et d'assistance mutuelle entre autorités européennes, tel que proposé par la Commission européenne afin de compenser la perte de compétences des autorités et l'allègement des formalités préalables. Ces mécanismes, tels qu'actuellement envisagés, semblent lourds et trop limités pour garantir une information et une coopération suffisante entre les autorités. Par exemple, il n'est pas prévu clairement qu'une faille de sécurité notifiée à l'autorité de l'établissement principal et impactant les citoyens d'autres États membres soit portée à la connaissance des autres autorités impactées. De même, en cas de consultation de l'autorité de l'établissement principal sur des traitements à risques, tel que les traitements biométriques, déployés dans toute l'Europe.

Ce dispositif proposé, qui conduit à la concentration de l'activité de régulation entre les mains d'un nombre très limité d'autorités, encouragera de plus les pratiques de « forum shopping » pour les traitements ayant pourtant un impact immédiat sur notre territoire, notamment ceux réalisés par les grands acteurs de l'Internet.

En effet, au sein de l'Union européenne, cette solution favorisera l'établissement d'entreprises vers les États membres dont les autorités de protection des données personnelles privilégient une approche plus « souple » (principalement les autorités anglo-saxonnes et nordiques).

Certains pays, comme l'Irlande, ayant également mis en place une politique fiscale particulièrement attractive, seront donc économiquement et politiquement plus attrayants que la France, réputée plus stricte. Ces quelques autorités disposent aujourd'hui, de surcroît, de peu de moyens financiers et humains : elles n'auront donc pas les ressources nécessaires pour assumer de telles responsabilités. Au total, une telle réforme favorisera la concurrence intra-communautaire et aura donc, de fait, des conséquences négatives sur le niveau de protection des citoyens européens.

Enfin, cette révision pèsera lourdement sur la compétitivité économique de la France au niveau européen, mais également sur l'attractivité du territoire communautaire par rapport aux autres grandes zones économiques de la planète.

Face à la concurrence très forte que se livrent aujourd'hui l'Union européenne et l'ensemble des zones économiques mondiales, cette réforme, telle que l'envisage la Commission, peut fragiliser l'attractivité de l'Europe. En concentrant le pouvoir au sein des autorités les moins exigeantes, et en affaiblissant celui d'autorités plus vigilantes comme la CNIL, le système proposé par la Commission aboutira, de fait, à diminuer le niveau de protection des données personnelles des citoyens au sein de l'Union européenne, alors même qu'il lui permet justement d'attirer des entreprises demandeuses d'un cadre juridique particulièrement protecteur et qu'il répond aux inquiétudes actuelles des consommateurs. L'Union européenne perdra ainsi un atout et un argument économique déterminants face à ces nouveaux concurrents, au moment même où les États membres traversent une crise économique sans précédent et cherchent justement à renforcer l'attractivité de l'économie européenne et les atouts de celle-ci.

En second lieu, au-delà des conséquences évoquées ci-dessus liées à l'introduction du critère de l'établissement dans le texte, cette réforme aboutira à la concentration de pouvoirs considérables entre les mains de la Commission européenne, conduisant à encadrer très fortement le pouvoir des autorités nationales.

En effet, le projet de règlement prévoit que la Commission sera exclusivement compétente pour élaborer des lignes directrices en matière de protection des données personnelles et définir les modalités précises d'application des nouvelles dispositions. Par exemple, si le projet de révision instaure un droit à l'oubli pour les citoyens, il reviendra à la seule Commission européenne d'en préciser les conditions concrètes d'application, tant juridiques que techniques. Et cela concerne la plus

grande partie des dispositions de cette révision. Sans vouloir remettre en cause les compétences des services de la Commission, sans doute serait-il plus cohérent et efficace de mieux y associer les autorités nationales de protection qui bénéficient d'une véritable expertise sur ces sujets techniques et sensibles grâce à leurs expériences respectives.

Enfin, en troisième lieu, dans une économie mondialisée où les données circulent à travers la planète, l'encadrement et la sécurité des transferts internationaux sont une priorité pour garantir aux citoyens un haut niveau de protection de leurs droits. Si la Commission européenne semble sensible à cette exigence, la possibilité qui sera désormais offerte aux responsables de traitement de mettre en œuvre certains transferts de données en dehors de l'Union européenne, en auto-évaluant les conditions de sécurité de ces échanges, fait peser un risque important sur les données personnelles de nos concitoyens. Il est absolument indispensable que les autorités nationales demeurent compétentes pour autoriser ces transferts, après un contrôle attentif des modalités de mise en œuvre de ces échanges.

Pour toutes ces raisons, en alternative à ce projet qui devra encore obtenir l'accord des différents gouvernements et du Parlement européen, d'autres solutions doivent être privilégiées pour atteindre les objectifs de simplification et d'harmonisation des règles, tout en préservant les compétences des autorités et un haut niveau de protection des droits des citoyens.

Ainsi, l'Assemblée nationale se félicite, par cette proposition de résolution, de certaines dispositions de ce projet de règlement qui consacreront de nouveaux droits pour les citoyens, comme le droit à l'oubli, ou le droit à la portabilité des données. Elle souligne également le renforcement des règles de recueil du consentement, l'augmentation conséquente des sanctions financières en cas de non-respect des dispositions légales...

Cependant, si toutes ces dispositions sont à saluer, il n'en demeure pas moins que d'autres dispositions sont aujourd'hui particulièrement inquiétantes et porteuses de conséquences politiques, économiques et juridiques considérables, contre lesquelles l'Assemblée nationale doit se prononcer par l'adoption de cette proposition de résolution européenne.

Aussi, il est indispensable que les autorités nationales de protection conservent toutes leurs compétences dès lors qu'un traitement cible spécifiquement les citoyens de ce pays, quelque soit le territoire sur lequel se situe l'établissement principal de ce responsable de traitement. Il est

également indispensable qu'une coopération élargie se mette en place entre les autorités de protection sur l'ensemble des sujets d'intérêt commun, à travers une gouvernance plus participative.

Les règles applicables aux transferts internationaux de données doivent également être renforcées pour préserver les pouvoirs de contrôle et d'autorisation a priori des autorités, de même que la répartition des pouvoirs entre la Commission européenne et les autorités nationales de protection doit être revue.

Devant un projet de réforme de cette ampleur, l'Assemblée nationale doit réaffirmer unanimement son engagement sur ces questions, comme elle a déjà eu l'occasion de le faire à de nombreuses reprises. Si elle soutient les objectifs annoncés par la Commission européenne en matière de modernisation, d'harmonisation et de simplification des règles applicables, elle doit appeler à des solutions plus protectrices des droits de nos concitoyens.

Les données personnelles des citoyens ne constituent pas seulement un enjeu économique dont il conviendrait d'optimiser la rentabilité. Leur protection et l'encadrement de leurs traitements représentent avant tout une question de libertés individuelles absolument fondamentales pour nos concitoyens.

Un engagement de la représentation nationale sur cette question constituera un message politique fort adressé aux citoyens français et aux instances européennes, en faveur d'une révision du cadre juridique communautaire plus respectueuse des droits des citoyens : c'est le sens de cette proposition de résolution européenne.

PROPOSITION DE RÉSOLUTION EUROPÉENNE

Article unique

- ① L'Assemblée nationale,
- ② Vu l'article 88-4 de la Constitution,
- ③ Vu l'article 151-5 du Règlement de l'Assemblée nationale,
- 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 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,
- ⑦ Vu la loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
- ⑧ Vu la communication de la Commission européenne COM(2010) 609 final, intitulée « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »,
- ⑨ Vu 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 COM(2012) 11/4,
- ⑩ 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 ;
- ⑪ 2. Soutient les objectifs annoncés par la Commission européenne dans sa communication du 4 novembre 2010 concernant la révision du cadre

juridique européen en matière de protection de la vie privée et des données personnelles ;

- ⑫ 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 ;
- ⑬ 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 ;
- ⑭ 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 ;
- ⑮ 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 ;
- ⑯ 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 pour celles publiées sur les réseaux sociaux, dans un format électronique qui permette leur réutilisation sur d'autres supports ;
- ⑰ 8. Défend la proposition de la Commission 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 désormais plus être assimilés à un consentement implicite ;
- ⑱ 9. Soutient la désignation obligatoire de correspondants informatique et libertés au sein des administrations publiques et des entreprises de plus de 250 salariés, telle que proposée par la Commission européenne. Cette disposition, particulièrement attendue par certaines autorités de protection

européenne, 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 ;

- ⑲ 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 ;
- ⑳ 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 ;
- ㉑ 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 ;
- ㉒ 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 traitements de données particulièrement sensibles, comme les données génétiques, biométriques, ou les données de santé, réduisant considérablement les contrôles a priori sur ces traitements à risques. 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 risques ;
- ㉓ 14. Regrette la concentration de pouvoirs considérables entre les mains de la Commission européenne, au dépend 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 ;
- ㉔ 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 transferts, par les responsables de traitement eux-mêmes, conduirait à une baisse considérable du niveau de protection des droits des citoyens ;

- ②⑤ 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.
- ②⑥ 17. Souhaite l'élaboration d'instruments internationaux pour la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui permettrait, au-delà du cadre européen, de mieux garantir le respect des droits à la protection des données et à la vie privée.

