N° 4325

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 7 février 2012.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES[1]
SUR LA PROPOSITION DE RESOLUTION EUROPEENNE (n° 4227)
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,**

ET PRÉSENTÉ

PAR M. Philippe GOSSELIN,

Député

[1] *La composition de cette Commission figure au verso de la présente page.*

La Commission des affaires européennes est composée de : M. Pierre Lequiller, *président* ; MM. Michel Herbillon, Jérôme Lambert, Didier Quentin, Gérard Voisin *vice-présidents* ; M. Jacques Desallangre, M^me^ Marietta Karamanli, MM. Francis Vercamer *secrétaires ;* M. Alfred Almont, M. Patrick Bloche, M^me^ Monique Boulestin, MM. Pierre Bourguignon, Yves Bur, Patrice Calméjane, Christophe Caresche, Philippe Cochet, Jean-Yves Cousin, Bernard Deflesselles, Lucien Degauchy, Michel Diefenbacher, Jean Dionis du Séjour, Marc Dolez, Daniel Fasquelle, Pierre Forgues, M^me^ Marie-Louise Fort, MM. Jean-Claude Fruteau, Jean Gaubert, Hervé Gaymard, Guy Geoffroy, M^mes^ Annick Girardin, M. Philippe Gosselin, Anne Grommerch, Pascale Gruny, Elisabeth Guigou, Danièle Hoffman-Rispal, MM. Régis Juanico, Robert Lecou, Michel Lefait, Lionnel Luca, Philippe Armand Martin, Jean-Claude Mignon, Pierre-Alain Muet, Jacques Myard, Michel Piron, Valérie Rosso-Debord, Odile Saugues, MM. André Schneider, Philippe Tourtelier.

SOMMAIRE

Pages

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 Etats 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 depuis l'adoption de la directive en 1995. Les données personnelles des citoyens ne sont plus seulement contenues dans des fichiers mis en place par les Etats ou les administrations, mais sont désormais traitées par différents acteurs publics et privés.

A 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, à l'informatique en nuage (« *cloud coumputing* ») 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 européen 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 une proposition de règlement pour l'ensemble des matières relevant de la directive de 1995, les questions relevant de l'ancien troisième pilier (coopération policière et judiciaire en matière pénale) faisant l'objet d'une proposition de directive.

L'Union européenne est donc à un moment charnière de sa politique de protection de la vie privée des résidents 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 et résidents européens.

I. LE CADRE EUROPÉEN DE PROTECTION DES DONNÉES

Il convient de distinguer la législation applicable au sein de l'Union européenne des conventions, plus générales, signées dans le cadre du Conseil de l'Europe.

A. La directive de 1995

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, constitue le socle de la législation communautaire en matière de protection des données. La directive ne s'applique pas à la protection des données en matière de coopération judiciaire pénale et de coopération policière, qui relevaient à l'époque du troisième pilier de l'Union, pour lequel la décision-cadre de 2008 a été élaborée[(2)]. Les fichiers dits « de souveraineté » ne relèvent donc pas de la directive de 1995.

Il convient de souligner que la directive de 1995 est très largement inspirée du droit français et de la loi « informatique et libertés » du 6 janvier 1978[(3)]. La législation française a, à cet égard, fait figure de pionnière et a devancé l'élaboration de normes au niveau européen. Il convient également de noter la stabilité du texte français, qui est remarquable et notamment liée à sa neutralité technologique.

La directive du 24 octobre 1995 prévoit que chaque Etat membre applique les dispositions de son droit national au traitement de données (article 4) :

- lorsque celui-ci est effectué dans le cadre des activités d'un établissement situé sur le territoire de l'Etat membre ;

- si le responsable du traitement n'est pas établi sur le territoire de l'Etat membre, mais en un lieu où sa loi nationale s'applique en vertu du droit international public ;

---

(2) 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.

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

- si le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt à des moyens situés sur le territoire de l'Etat membre à des fins de traitement des données à caractère personnel.

L'article 6 dispose que les données à caractère personnel doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, explicites et légitimes. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, exactes et, si nécessaire, mises à jour. Elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées. Le responsable du traitement est tenu d'assurer le respect de ces conditions.

Le traitement des données ne peut être effectué que si la personne concernée a indubitablement donné son consentement (ou s'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou à la sauvegarde de l'intérêt vital de la personne, ou à l'exécution des missions d'intérêt public relevant de l'exercice de l'autorité publique, ou encore s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement).

Le traitement des données dites sensibles, c'est-à-dire celles qui peuvent révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la santé et à la vie sexuelle, est en principe interdit. Toutefois, la directive prévoit que, si la personne a donné son consentement explicite, le traitement peut intervenir. Des dérogations sont également prévues en matière de traitement s'agissant du droit du travail, lorsqu'il est question de défendre les intérêts vitaux de la personne ou encore pour les activités légitimes des fondations ou associations à but non lucratif ayant, par exemple, une finalité politique ou religieuse, à condition que le traitement ne concerne que les membres de l'organisme ou des personnes entretenant avec lui des contacts réguliers et que les données ne soient pas communiquées à des tiers sans le consentement des personnes. Une dérogation est également prévue pour les données manifestement rendues publiques par la personne concernée. Par ailleurs, le principe d’une interdiction du traitement des données sensibles ne s’applique pas non plus en matière de médecine préventive, de diagnostics médicaux et de gestion des services de santé. Les Etats membres peuvent également prévoir, pour un motif d'intérêt public important, d'autres dérogations.

Par ailleurs, des exemptions particulières doivent être prévues pour les traitements de données personnelles effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, en vue de concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

L’article 10 prévoit que le responsable du traitement doit fournir des informations à la personne auprès de laquelle il collecte les données (responsable du traitement, finalités du traitement, destinataires des données, caractère facultatif ou non de la réponse aux questions posées, droit d'accès aux données).

La personne dont les données sont soumises à un traitement dispose d'un droit d'accès à ces données (article 12) qui doit être possible sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs.

Les principes relatifs à la qualité des données, à l'information de la personne concernée, au droit d'accès et à la publicité des traitements peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'Etat, la défense, la sécurité publique, la poursuite d'infractions pénales, un intérêt économique ou financier important d'un Etat membre ou de l'UE ou la protection de la personne concernée (article 13).

La personne dispose d'un droit d'opposition, si elle fait valoir des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que les données qui la concernent fassent l'objet d'un traitement. La personne doit également pouvoir s'opposer, sur simple demande et gratuitement, au traitement de ces données à des fins de prospection.

La directive proscrit également que les décisions produisant des effets juridiques ou affectant une personne de manière significative soient prises sur le seul fondement d'un traitement automatisé de données (notamment pour évaluer certains aspects de la personnalité, le rendement professionnel ou la fiabilité d’un salarié).

Le responsable du traitement à l'obligation de garantir la confidentialité ainsi que la sécurité du traitement et doit prendre toutes les mesures appropriées pour protéger les données contre la destruction accidentelle ou illicite, la perte, l'altération, la diffusion ou encore l'accès non autorisé aux données. Lorsqu'il choisit un sous-traitant pour effectuer le traitement, le responsable du traitement doit s'assurer que celui-ci apporte des garanties suffisantes.

La directive prévoit en son article 18 une obligation de notification à l'autorité de contrôle de la protection des données (la CNIL en France), préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé de données à caractère personnel. Certains aménagements peuvent être prévus afin de simplifier les obligations de notification, notamment lorsque les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées. Des examens préalables sur les risques éventuels au regard des droits et libertés des personnes sont effectués par l'autorité de contrôle après réception de la notification. La publicité des traitements doit être assurée et les autorités de contrôle doivent tenir un registre des traitements notifiés.

Sans préjudice d'un recours possible par voie administrative, notamment auprès d'une autorité de contrôle, toute personne doit disposer d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par la directive. Lorsqu'une personne subit un préjudice du fait d'un traitement illicite ou de toute action incompatible avec les prescriptions de la directive, la personne a le droit d'obtenir réparation de la part du responsable du traitement.

La question du transfert des données à caractère personnel vers les pays tiers a également une importance considérable. Le principe posé est que les Etats membres doivent s'assurer que le transfert de données personnelles vers un pays tiers ne peut se faire que si le pays tiers en question assure un niveau de protection des données adéquat. Le caractère adéquat du niveau de protection s'apprécie en considération de la nature des données, de la finalité et de la durée du traitement, du pays d'origine et de destination finale, des règles de droit en vigueur dans le pays en question ainsi que des règles professionnelles et des mesures de sécurité qui sont appliquées. La Commission européenne constate le caractère adéquat[4] ou non du niveau de protection dans un Etat tiers.

Un certain nombre de dérogations au principe selon lequel le transfert de données vers un Etat n'assurant pas un niveau adéquat de protection est interdit sont posées par l'article 26. Ainsi, le transfert est possible si la personne concernée a indubitablement donné son consentement, si le transfert est nécessaire à l'exécution d'un contrat auquel la personne est partie ou à la conclusion d'un contrat dans son intérêt, si le transfert est nécessaire pour la sauvegarde d'un intérêt public important ou pour la sauvegarde de l'intérêt vital de la personne ou encore si le transfert intervient au départ d'un registre public qui est ouvert à la consultation du public ou de toute personne justifiant un intérêt légitime. Un Etat membre peut également autoriser un transfert lorsque le responsable du traitement offre des garanties suffisantes au regard des droits fondamentaux des personnes. Dans ce dernier cas, l'Etat membre informe la Commission européenne et les autres Etats membres des autorisations qu'il a accordées. Ces derniers peuvent s'y opposer. Par ailleurs, lorsque la Commission européenne décide que certaines clauses contractuelles types présentent des garanties suffisantes, alors les Etats membres se conforment à la décision de la Commission européenne[5].

Enfin, la directive prévoit qu'une ou plusieurs autorités publiques doivent être chargées dans chaque Etat membre de surveiller l'application, sur son territoire, des mesures prises en application de la directive (article 28). Ces

---

[4] Liste des pays ayant fait l'objet d'une décisions d'adéquation : Andorre, Argentine, Australie, Canada, Suisse, les Îles Féroé, Guernesey, Israël, l'Île de Man et Jersey. Il faut également signaler que, les entreprises localisées aux États-Unis et adhérant aux règles des principes de la « sphère de sécurité » (Safe Harbor) sont considérées comme assurant un niveau de protection adéquat.

[5] Décision de la Commission européenne du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil.

autorités doivent exercer en toute indépendance les missions dont elles sont investies. Elles sont consultées lors de l'élaboration des mesures réglementaires ou administratives entrant dans leur champ de compétences. Chaque autorité doit notamment disposer de pouvoirs d'investigation (pouvoir d'accéder aux données et de recueillir toutes les informations nécessaires), de pouvoirs effectifs d'intervention (avis préalable à la mise en œuvre de traitement, possibilité d'ordonner le verrouillage, l'effacement ou la destruction de données ou d'interdire un traitement, pouvoir d'adresser un avertissement, pouvoir de saisir les parlements nationaux ou d'autres institutions politiques) et du pouvoir d'ester en justice en cas de violation de la réglementation ou de porter ces violations à la connaissance de l'autorité judiciaire. Les autorités de protection des données peuvent être saisies par toute personne (ou par une association) d'une demande relative à la protection de ses droits et libertés.

La directive institue également un groupe de protection des personnes à l'égard du traitement des données personnelles (article 29), dit « groupe de l'article 29 » ou « G29 », qui réunit les représentants des autorités de contrôle des Etats membres ainsi qu'un représentant de la Commission européenne et un représentant des autorités créées par les institutions et organismes communautaires (lesquels ne sont pas soumis aux dispositions de la directive mais relèvent d'une réglementation propre)[(6)].

Le cadre juridique européen a été complété par la directive 2002/58/CE du 12 juillet 2002, dite directive « vie privée et communications électroniques »[(7)], relative au traitement de données à caractère personnel dans le cadre de la fourniture de services de télécommunications accessibles au public dans l'union européenne. La directive a prévu que les données de connexion (logs) doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication. Les courriers électroniques envoyés par des « *systèmes automatisés sans intervention humaine* » (spams) ne peuvent viser que des personnes ayant donné leur consentement préalable, et ayant exercé un « *opt-in* ». L'utilisation de témoins de connexions ou « *cookies* » est permise à condition qu'une information « claire et complète » soit transmise à l'abonné, notamment sur les finalités du traitement, ce dernier devant avoir la possibilité de les refuser.

Compte tenu des disparités de transposition et des difficultés d'harmonisation des législations entre les Etats membres, une nouvelle directive 2006/24/CE du 15 mars 2006 sur la conservation des données générées ou traitées

---

[(6)] Il convient de noter que les données personnelles traitées par les instances communautaires relèvent du règlement 45/2001/CE du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et les organes de l'Union européenne et à la libre circulation des données.

[(7)] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

dans le cadre de la fourniture de services de communications électroniques a été adoptée[8]. Les Etats membres ayant légiféré sur la conservation des données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales de manière très disparate, il est apparu que les entraves au marché intérieur des communications électroniques nécessitaient de fixer un nouveau cadre européen. En effet, les fournisseurs de services devaient jusqu'alors satisfaire à des exigences différentes s'agissant des types de données relatives au trafic et à la localisation a conserver ainsi que des conditions et des durées de conservation. La directive vise à harmoniser leurs obligations en vue de garantir la disponibilité des données pour la recherche, la détection et la poursuite d'infractions graves. Les catégories de données sont listées et une durée de conservation comprise entre six mois et deux ans est instituée.

Enfin, la directive 2009/136/CE du 25 novembre 2009, applicable aux fournisseurs de services de communications électroniques, impose aune obligation de notification des violations des données à la CNIL (et aux utilisateurs pour les cas les plus graves). L'information relative à l'installation de « cookies » sur les ordinateurs personnels est renforcée.

B. Le Conseil de l'Europe et la convention n° 108

L'article 8 de la convention européenne des droits de l'homme dispose que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

La convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981, dite convention n° 108 a pour but de garantir, « *sur le territoire de chaque partie, à toute personne physique, quelle que soit sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant* » (article premier). La convention 108 du Conseil de l'Europe a été le premier traité international contraignant en la matière et 41 Etats membres du Conseil de l'Europe y sont parties, parmi lesquels l'ensemble des Etats membres de l'Union européenne.

Elle prévoit que les données à caractère personnel faisant l'objet d'un traitement automatisé sont :

« - obtenues et traitées loyalement et licitement ;

---

[8] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

- enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ;

- adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;

- exactes et si nécessaire mises à jour ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. »

Les données sensibles ne peuvent faire l'objet d'un traitement automatisé à moins que des dispositions spécifiques ne soient prises. Des mesures de sécurité doivent être prises contre la destruction des données (accidentelle ou non autorisée), leur perte, ainsi que contre l'accès, la modification ou la diffusion non autorisés. Les personnes concernées bénéficient d'un droit à l'information, à la rectification ou à l'effacement des données ainsi que d'un droit au recours. Les dérogations possibles sont strictement encadrées et visent la protection de la sécurité de l'Etat, la sûreté publique, les intérêts monétaires de l'Etat ou la répression des infractions pénales, ainsi que la protection de la personne concernée et des droits et libertés d'autrui.

Son protocole additionnel, concernant les autorités de contrôle et les flux transfrontières de données, établi à Strasbourg le 8 novembre 2001, dispose en son article premier qu'une autorité indépendante doit être chargée de veiller au respect des mesures appliquant les principes énoncés dans la convention et dans son protocole additionnel. « *Ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne*. »

S'agissant des flux transfrontières de données vers un destinataire n'étant pas soumis à la juridiction d'une partie à la convention, le transfert ne peut être effectué que si l'Etat ou l'organisation assure un niveau de protection adéquat pour le transfert considéré.

Dans la résolution 1843 (2011) adoptée le 7 octobre 2011, relative à la protection de la vie privée et des données à caractère personnel sur l'Internet et des médias en ligne, l'assemblée parlementaire du Conseil de l'Europe se félicite que la convention n° 108 ait été signée et ratifiée par presque tous les Etats membres du Conseil de l'Europe, à l'exception « regrettable » de l'Arménie, de la fédération de Russie, de Saint-Marin et de la Turquie. « *L'assemblée déplore que l'absence de normes juridiques mondialement acceptées sur la protection des données concernant les réseaux et les services fondés sur les TIC débouche sur une insécurité juridique et contraigne les tribunaux nationaux à combler ce vide, au cas par cas, en interprétant des lois internes à la lumière de l'article 17 du pacte*

international relatif aux droits civils et politiques et de l'article huit de la Convention européenne des droits de l'homme. » L'assemblée appuie les démarches entreprises par les autorités indépendantes de protection des données en matière de coopération internationale, et tout particulièrement les résolutions adoptées à Madrid en 2009 et à Jérusalem en 2010. L'assemblée appelle l'Union européenne à continuer de soutenir une large adhésion à la convention n° 108 et à son protocole additionnel et à en devenir elle-même partie.

La Cour européenne des droits de l'Homme a rappelé, dans sa jurisprudence, l'importance fondamentale de la protection des données à caractère personnel pour le respect du droit à la vie privée, tel que garanti par l'article 8 de la convention européenne des droits de l'Homme. Se référant à la convention 108, elle en a retiré des critères permettant de juger d'une atteinte à ce droit (CEDH, arrêt Z contre Finlande, 25 février 1997). Par ailleurs, la Cour peut également partir du principe que la convention impose des obligations aux Etats parties à la convention et a pu juger un Etat comme étant responsable de la violation du droit à la vie privée par des parties privées entre elles (CEDH, arrêt Von Hannover contre Allemagne, 24 juin 2004 et I. Contre Finlande, 17 juillet 2008, s'agissant du respect de la confidentialité des données relatives à la santé).

Au-delà de cet instrument, il n'existe pas d'instrument juridique contraignant de dimension internationale au-delà de l'Union européenne.

II. LA NECESSAIRE RÉFORME DE LA DIRECTIVE DU 24 OCTOBRE 1995

L'entrée en vigueur du traité de Lisbonne, le 1er décembre 2010, a donné force contraignante à la Charte des droits fondamentaux, qui dispose en son article 8 que toute personne a droit à la protection des données à caractère personnel la concernant. Par ailleurs, le nouvel article 16 du traité sur le fonctionnement de l'Union européenne définit les règles d'adoption des textes européens permettant de garantir le droit à la protection des données personnelles.

Article 8 de la Charte européenne des droits fondamentaux

Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. 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. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Article 16 TFUE

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

Depuis 2009, la Commission européenne a organisé des consultations publiques sur la réforme du cadre européen de protection des données. Dans sa communication du 4 novembre 2010, relative à une approche globale de la protection des données à caractère personnel dans l'Union européenne (COM (2010) 609), la Commission européenne exposait les principaux thèmes de réforme.

Dans sa communication du 25 janvier 2012 « *Protection de la vie privée dans un monde en réseaux. Un cadre européen relatif à la protection des données, adaptée aux défis du XXI*e *siècle* », la Commission européenne rappelle la rapidité des évolutions technologiques et la mondialisation qui ont modifié en profondeur l'utilisation, la collecte, la consultation et les transferts des données à caractère personnel. Les 250 millions d'internautes européens utilisent de manière massive les réseaux sociaux et les réseaux de stockage à distance de données. Les données à caractère personnel sont exploitées par les entreprises et précieuses pour leurs activités économiques. Avec l'entrée en vigueur du traité de Lisbonne, et la force juridique contraignante consacrée à la charte des droits fondamentaux, la protection des données repose notamment sur l'article huit de la charte des droits fondamentaux et sur l'article 16 du traité sur le fonctionnement de l'Union européenne. Par ailleurs, le programme de Stockholm met en avant le besoin pour l'Union de disposer d'un régime complet de protection des données personnelles, conformément aux traités.

La confiance des consommateurs est un pré requis nécessaire à la croissance économique et à la compétitivité des entreprises. C'est pourquoi la Commission européenne a souhaité instituer des règles « *cohérentes et modernes applicables dans l'ensemble de l'Union* [qui] *s'imposent pour permettre la libre circulation des flux de données d'un Etat membre à l'autre. Les entreprises ont besoin de règles claires et uniformes qui garantissent la sécurité juridique et allègent le plus possible leurs charges administratives* ». C'est pourquoi elle propose de renforcer la dimension « marché intérieur » de la réglementation.

La directive de 1995 a été adoptée à une époque où l'Internet n'en était qu'à ses balbutiements. Elle ne permet ni un degré d'harmonisation suffisant, ni l'efficacité nécessaire dans l'environnement numérique actuel. La Commission européenne a donc déposé une proposition de règlement tendant à remplacer la directive de 1995 et instituant un cadre général de l'Union en matière de protection des données, ainsi qu'une proposition de directive, qui remplacerait la décision-cadre de 2008, relative à la protection des données traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière, ainsi que d'activités judiciaires connexes.

Seule la réforme de la directive du 24 octobre 1995 sera traitée ici.

A. Des avancées très attendues

Cette proposition est porteuse de nombreuses avancées, attendues et nécessaires. Ainsi, les citoyens se verraient reconnaître un droit à l'oubli numérique, les règles de recueil de leur consentement seraient renforcées, les correspondants informatiques et libertés seraient rendus obligatoires dans les administrations publiques et certaines entreprises ; ces dernières devraient 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 seraient considérablement renforcées, *etc*. 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.

Afin d'assurer une réelle harmonisation des droits nationaux ainsi qu'une protection uniforme des droits à la vie privée et à la protection des données dans l'Union, la Commission européenne propose de réformer la directive de 1995 par un règlement, qui sera donc d'application directe et ne nécessitera pas de transposition. Un règlement est également jugé nécessaire aux acteurs économiques afin de garantir la sécurité juridique, la transparence des règles et de limiter les entraves au marché intérieur.

La proposition de règlement concernerait les personnes physiques résidant dans l'Union, indépendamment de leur nationalité.

Le règlement ne couvrirait pas le traitement de données à caractère personnel par les institutions et organes de l'Union, ni celui fait par les Etats membres dans le contexte de leurs activités liées à la politique étrangère et de sécurité commune de l'Union ou à la coopération policière et judiciaire pénale. Il ne s'appliquerait pas aux traitements de données effectués par une personne physique, qui seraient exclusivement personnels ou domestiques, sans but lucratif, et sans lien avec une activité professionnelle commerciale.

Le règlement serait applicable, non seulement pour tout traitement intervenant dans le cadre des activités d'un établissement situé sur le territoire de l'Union, mais aussi, si le responsable du traitement n'est pas établi dans l'Union, dès lors que le traitement concerne les personnes résidant dans l'Union lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou à l'observation de leur comportement.

La liste des données à caractère personnel sensibles serait élargie aux données génétiques et aux données relatives à des condamnations pénales.

En principe, les données sensibles ne devraient pas faire l'objet d'un traitement, à moins que la personne concernée n'y consente expressément. Toutefois, les dérogations à cette interdiction seraient prévues lorsque les données ont manifestement été rendues publiques par la personne ou pour tenir compte de besoins spécifiques lorsque le traitement a lieu dans le cadre du droit du travail ou d'activités légitimes de certaines associations ou fondations. Par ailleurs le traitement de telles catégories de données pourrait résulter de la loi, dans le cas où des raisons d'intérêt général le justifient, sous réserve de garanties appropriées. Le traitement de telles données serait possible à des fins de santé publique (protection de la santé, protection sociale, gestion des services de santé). Les finalités statistiques et de recherche, historique ou scientifique, sont également prévues.

1. Le droit à l'oubli numérique

Le caractère massif des échanges de données à caractère personnel, l'internationalisation de ces échanges, la marchandisation des données personnelles et l'attrait commercial que suscitent les informations nominatives, les nouvelles possibilités technologiques qui permettent d'accroître les capacités de stockage et de conservation des données dans des proportions auparavant inimaginables sont autant d'éléments qui ont fait naître la revendication d'un droit à l'oubli.

Comme le soulignait le rapport d'information n° 3560 de Messieurs Patrick Bloche et Patrice Verchère « *Révolution numérique et droits de l'individu : pour un citoyen libre et informé* », le droit à l'oubli est au croisement de trois préoccupations :

- savoir que les données à caractère personnel collectées ne sont pas conservées au-delà de la période strictement nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées ;

- avoir la possibilité d'effacer les informations qui ont été mises en ligne sur une plate-forme de partage, telle que Facebook ;

- avoir l'assurance que les informations rendues publiques par soi-même ou par un tiers et disponibles sur Internet ne seront pas facilement accessibles au-delà d'un certain délai.

Les travaux menés par la mission d'information précitée ont démontré qu'invoquer l'oubli sur les réseaux pourrait bien constituer une forme de gageure puisqu'un même contenu, une fois mis en ligne, peut-être dupliqué à l'infini et donc remis en ligne même s'il a été effacé par l'auteur d'origine. Par ailleurs, il est bien souligné que le modèle de l'économie numérique repose sur la gratuité des réseaux, laquelle est bien entendu compensée par la valorisation des données personnelles qui sont utilisées pour la publicité. « *La consécration d'un tel droit absolu à l'oubli sur Internet risquerait de rompre le point d'équilibre actuel entre le nécessaire financement de l'économie numérique, dont le dynamisme soutient incontestablement la croissance et l'activité de notre pays, et l'indispensable protection de la vie privée dans la société d'information*. »

Le rapport préconise davantage, dans un souci de réalisme, d'améliorer en amont l'information de l'internaute et de lui offrir les outils lui permettant d'assurer un meilleur contrôle de ces données personnelles. Toutefois, s'agissant des difficultés spécifiques rencontrées sur les réseaux sociaux, un droit à l'oubli dédié et adapté à ces derniers devrait, selon les rapporteurs, être envisagé avec un droit effectif à l'effacement des données (et non un simple droit à la désactivation du profil), la garantie d'une procédure simple et accessible permettant d'effacer l'intégralité de ses données ou de les récupérer pour les réutiliser, et le principe

d'un effacement des données d'un profil après un certain délai si aucun usage n'en est fait.

La proposition de règlement de la Commission européenne prévoit que « *toute personne devrait avoir le droit de faire rectifier des données à caractère personnel la concernant, et disposer d'un « droit à l'oubli numérique » lorsque la conservation de ces données n'est pas conforme au présent règlement. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données soient effacées et ne soient plus traitées, lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant ou encore, lorsque le traitement de leurs données à caractère personnel n'est pas conforme au présent règlement. Ce droit est particulièrement important lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et donc mal informée des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'Internet. Toutefois, la conservation des données devrait être autorisée lorsqu'elle est nécessaire à des fins statistiques ou de recherche historique ou scientifique, pour des motifs d'intérêt général dans le domaine de la santé publique, ou à l'exercice du droit à la liberté d'expression, si elle est requise par la loi ou s'il existe une raison de limiter le traitement des données au lieu de les effacer.*

(54) Afin de renforcer le « droit à l'oubli numérique » dans l'environnement en ligne, le droit à l'effacement des données devrait en outre être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données, ou toute copie ou reproduction de celles-ci. Afin d'assurer cette information, le responsable des données devrait prendre toutes les mesures raisonnables, y compris les mesures techniques, à l'égard des données dont la publication lui est imputable. En ce qui concerne la responsabilité de la publication de données à caractère personnel par un tiers, elle devrait être imputée au responsable du traitement lorsqu'il a lui-même autorisé le tiers à l'effectuer » (considérants 53 et 54).

Le droit à l'oubli serait consacré à l'article 17 de la directive.

Le rapporteur estime que la mise en œuvre d'un droit général à l'oubli pourrait bien se révéler impraticable. Il souhaiterait que, dans un souci de réalisme, le droit à l'oubli soit en priorité imposé aux réseaux sociaux, car ces derniers ont fait naître ces dernières années des problématiques très spécifiques en termes de protection des données personnelles. Il convient également de souligner que la proposition de règlement ne confère pas de manière claire la possibilité de

demander la suppression de données mises en ligne par un tiers. Ce droit devrait être garanti.

L'article 18 consacrerait le droit à la portabilité des données lorsque les données font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé. La personne concernée aurait le droit d'obtenir auprès du responsable du traitement une copie des données, ce qui permettrait leur réutilisation.

2. Le renforcement du recueil du consentement

Le droit à l'information serait renforcé. La personne concernée devrait être informée de l'existence d'un traitement, de ses finalités, de la durée de conservation des données, de l'existence de droits d'accès aux données, de rectification ou d'effacement, ainsi que du droit à introduire une réclamation. Ces informations devraient être fournies à la personne au moment où ses données sont recueillies ou, si la collecte n'a pas lieu auprès de la personne concernée, dans un délai raisonnable. Lorsque les données peuvent être légitimement divulguées à un autre destinataire, la personne concernée devrait être informée lorsque les données sont divulguées pour la première fois (sauf si la divulgation est expressément prévue par la loi ou si l'information de la personne se révèle impossible ou exige des efforts disproportionnés. Seraient ici visés les problèmes d'information dans le cas de traitement à des fins statistiques ou de recherche historique.).

Toute personne devrait avoir le droit d'accéder aux données qui la concernent. La personne pourrait également se faire communiquer l'identité des destinataires, la logique qui sous-tend le traitement des données et les conséquences qu'il pourrait avoir, au moins en cas de profilage, sans toutefois porter atteinte au secret des affaires, ni à la propriété intellectuelle.

Lorsque des données sont traitées à des fins de *marketing* direct, la personne concernée devrait avoir le droit de s'opposer à ce traitement, sans frais et d'une manière simple et effective. Toute personne devrait avoir le droit de ne pas être soumise à une mesure fondée sur le profilage par traitement automatisé (sauf pour les mesures autorisées par la loi, appliquées dans le cadre de la conclusion ou de l'exécution d'un contrat ou si la personne a donné son consentement).

Pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement explicite, libre et informé de la personne concernée. La personne devrait disposer d'une véritable liberté de choix. Il ne saurait y avoir de consentement tacite ou passif car le consentement impliquerait une démarche active de la personne concernée. La charge de prouver que la personne a consenti au traitement de ses données à caractère personnel incomberait au responsable du traitement. Celle-ci aurait le droit de retirer son consentement à tout moment. En ce qui concerne les enfants de moins de 13 ans, la licéité du traitement nécessiterait que le consentement soit donné ou autorisé par

un parent de l'enfant ou par une personne qui en a la garde. Le responsable du traitement devrait s'efforcer raisonnablement d'obtenir un consentement vérifiable, compte tenu des moyens techniques disponibles.

3. Vers une responsabilité accrue des responsables de traitement

Il appartiendrait au responsable du traitement de prendre les mesures techniques et organisationnelles appropriées, tant au moment de la conception que de l'exécution du traitement. Les principes de la protection des données dès la conception (« *privacy by design* ») et de la protection des données par défaut seraient posés.

Lorsqu'un responsable du traitement n'est pas établi dans l'Union et traite des données à caractère personnel de résidents de l'Union, alors le responsable devrait désigner un représentant qui agirait pour son compte et devrait pouvoir être contacté par toute autorité de contrôle. Le responsable du traitement ou le sous-traitant devrait évaluer les risques inhérents au traitement et prendre les mesures nécessaires pour les atténuer.

La violation de données à caractère personnel faisant courir des risques importants, pouvant causer de graves pertes économiques et des dommages sociaux sérieux (parmi lesquels l'usurpation d'identité), dès lors que le responsable du traitement apprendrait qu'une telle violation s'est produite, il devrait en informer l'autorité de contrôle sans retard injustifié et, lorsque c'est possible, dans les 24 heures. Les personnes physiques concernées qui pourraient être affectées par la violation des données devraient également en être averties sans retard injustifié afin de pouvoir prendre les précautions qui s'imposent (cas dans lesquels la violation concerne les numéros de carte bancaire par exemple). La notification devra décrire la nature de la violation des données et formuler des recommandations à la personne afin d'atténuer les éventuels effets négatifs. A l'heure actuelle, il n'existe pas d'obligation de notification des violations des données, hormis pour les fournisseurs de services de communications électroniques. Il s'agirait donc d'une avancée importante.

La directive de 1995 prévoyait une obligation générale de notifier les traitements de données à caractère personnel. Or, la charge administrative et financière représentée par cette obligation paraît disproportionnée, sans pour autant permettre véritablement de protéger les données à caractère personnel. Des procédures et des mécanismes efficaces ciblant plutôt les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes, du fait de leur nature, leur portée ou de leur finalité, remplacerait cette obligation générale de notification. Une analyse d'impact devrait être réalisée par le responsable du traitement.

Si une étude d'impact fait état de risques particuliers pour les droits et libertés des personnes, l'autorité de contrôle devrait être consultée avant le début

de l'opération. Il en serait de même si le traitement appartient à la liste des traitements devant faire l'objet d'un contrôle préalable, définie par l'autorité de contrôle en fonction de la nature, de la portée et des finalités du traitement (articles 33 et 34).

Lorsqu'un traitement est réalisé dans le secteur public ou par une grande entreprise du secteur privé ou par une entreprise du secteur privé dont les activités de base impliquent des opérations de traitement exigeant un suivi régulier et systématique, un délégué à la protection des données devrait être désigné, qu'il soit ou non employé du responsable du traitement. Il devrait être en mesure d'exercer ses fonctions en toute indépendance (articles 35 à 37). Il pourrait être un salarié du responsable du traitement ou du sous-traitant, ou bien être employé sur la base d'un contrat de services. Ses éventuelles fonctions professionnelles devraient être compatibles avec la fonction de délégué à la protection des données, et ne pas entraîner de conflits d'intérêts. Il devrait disposer des compétences nécessaires à l'accomplissement de sa mission (techniques notamment). Un groupe d'entreprises pourrait désigner un délégué unique. Son mandat serait fixé pour deux ans au moins, renouvelables. Le cas d'un salarié désigné comme délégué à la protection des données soulèvera probablement des difficultés importantes. Ce point devra être étudié de près au cours des négociations. Ses fonctions seraient en effet assez larges et susceptibles de le placer dans une situation délicate vis-à-vis de son employeur, auquel il demeurerait lié par un lien de dépendance et de subordination (information et conseil auprès du responsable du traitement, contrôle de la mise en œuvre des règles internes, contrôle de l'application du règlement européen, contrôle de la documentation relative au traitement, vérification portant sur le fait qu'une analyse d'impact a été réalisée et que les demandes éventuelles de l'autorité de contrôle ont reçu une réponse, point de contact pour l'autorité de contrôle). En outre, le fait que la désignation du délégué à la protection des données soit obligatoire pourrait s'avérer contre-productif et ne pas produire d'effets bénéfiques en termes de diffusion d'une culture de protection des données.

La création de dispositifs de certification, de marques et de labels en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer le niveau de protection offert par les produits et services. L'élaboration de codes de conduite serait également encouragée (articles 38 et 39).

Des amendes plus lourdes devraient pouvoir être infligées par les autorités de contrôles (jusqu'à 2 % du chiffre d'affaires annuel mondial de l'entreprise pour les violations du règlement les plus graves). En France, les amendes sont plafonnées à 150 000 euros (l'article 47 de la loi de 1978 limite la sanction financière à 150 000 euros, ou 300 000 euros en cas de manquement réitéré dans les cinq années, à condition de ne pas excéder 5 % du chiffre d'affaires hors taxes du dernier exercice clos).

B. certaines propositions sont toutefois très problématiques

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

1. Le critère de l'établissement principal fait courir un risque élevé de nivellement par le bas des exigences en matière de protection des données

Le rapporteur estime que 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 Etats 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 conséquentes politiques importantes, puisqu'elle participera à un éloignement sensible des citoyens des autorités compétentes. Comment les résidents français pourront-ils en effet comprendre, et accepter, qu'une entreprise installée sur le territoire français, traitant des données personnelles de résidents 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 Etat membre.

Le rapporteur estime que c'est bien l'effectivité des droits institués par le règlement qui est ici en cause.

De plus, cette image technocratique sera également renforcée par le mécanisme de coopération et d'assistance mutuelle entre autorités européennes, tel qu'il est 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 résidents d'autres Etats membres soit portée à la connaissance des autres autorités impactées. Il en est de même, en cas de consultation de l'autorité de l'établissement principal sur des traitements à risques, tels 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 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. Au sein de l'Union européenne, cette solution favorisera l'établissement d'entreprises vers les Etats membres dont les autorités de protection des données personnelles privilégient une approche plus « souple » (principalement les autorités anglo-saxonnes et nordiques). En effet, quand bien même le règlement serait un instrument permettant une plus grande harmonisation qu'une directive, le risque de « *forum shopping* » n'en serait pas moins réel car la disparité de la mise en œuvre de la protection des données personnelles en Europe découle au moins autant des différences existant entre les droits des Etats membres que des différences d'approche retenues par les autorités de protection nationales. 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, de fait, des conséquences négatives sur le niveau de protection des citoyens européens.

Enfin, il convient de souligner que cette révision pourrait, à terme, peser 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. En effet, 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 européenne, pourrait finalement fragiliser l'attractivité de l'Europe pour un certain nombre d'entreprises. 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 européenne aboutira, de fait, à diminuer le niveau de protection des données personnelles des résidents 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 perdrait ainsi un atout et un argument économique déterminants face à ses concurrents, au moment même où les Etats membres traversent une crise économique sans précédent et

cherchent précisément à renforcer l'attractivité de l'économie européenne et ses atouts.

2. Des pouvoirs d'exécution excessifs confiés à la Commission européenne

Au-delà des conséquences évoquées ci-dessus liées à l'introduction du critère de l'établissement principal dans le texte, cette réforme aboutirait 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 européenne 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. Il s'agit là du recours devenu classique aux procédures dites de « comitologie », par lesquelles la Commission européenne se voit confier des pouvoirs d'exécution afin d'adopter des actes délégués visant à préciser les textes adoptés par le Conseil et le Parlement européen, assistée en cela par un comité regroupant des experts des Etats membres et un représentant de la Commission européenne, qui ne prend pas part aux votes du comité[(9)]. Il convient de veiller à ce que le pouvoir conféré au comité et à la Commission européenne ne déborde pas du cadre des seules compétences techniques d'exécution. La plus grande partie des dispositions de cette réforme sont concernées. Il est certes prévu que certaines délégations de pouvoir puissent être révoquées à tout moment par le Parlement européen ou le Conseil. En outre, pour les dispositions les plus importantes, les actes délégués n'entreraient en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé son opposition dans un délai de deux mois (pouvant être porté à quatre mois). Par ailleurs, en fonction de l'importance des actes, les décisions du comité peuvent s'imposer à la Commission européenne[(10)]. Toutefois, un tel recours quasi systématique aux actes délégués pour préciser la quasi-totalité des points du règlement parait de mauvaise méthode. Sans vouloir remettre en cause les compétences des services de la Commission, sans doute serait-il plus cohérent et efficace de mieux définir les choses au niveau du règlement et de mieux associer les autorités nationales de protection qui bénéficient d'une véritable expertise sur ces sujets techniques et sensibles grâce à leurs expériences respectives.

---

(9) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission.

(10) Article 5 du règlement 182/2011 précité.

3. Les transferts de données vers les Etats tiers ne seraient pas suffisamment contrôlés

En principe, un transfert de données à caractère personnel destiné à faire l'objet d'un traitement vers un pays tiers ou une organisation internationale ne serait possible que si la Commission européenne a constaté que le pays tiers ou un secteur de traitement de données dans ce pays tiers assure un niveau de protection adéquat. La Commission européenne prendrait en considération des éléments tels que la primauté du droit, la législation applicable, les règles professionnelles et les mesures de sécurité dans l'Etat, l'existence de droits effectifs et opposables, notamment pour les résidents de l'Union, l'existence et le fonctionnement effectif d'une autorité de contrôle ainsi que les engagements internationaux souscrits par le pays tiers. Lorsque la Commission européenne adopte une décision selon laquelle le pays tiers n'assure pas un niveau adéquat de protection, aucun transfert ne peut avoir lieu.

En l'absence de décision s'agissant du niveau de protection, le transfert ne serait possible que si le responsable du traitement respecte des règles d'entreprises contraignantes, telles qu'elles sont définies par le règlement (article 43), des clauses types de protection des données adoptées par la Commission européenne ou par une autorité de contrôle ou des clauses contractuelles liant le responsable du traitement et le destinataire des données et approuvées par une autorité de contrôle.

Dans le cas où aucune décision sur le caractère adéquat du niveau de protection n'a été prise par la Commission européenne et où il n'existe pas de garanties jugées appropriées, le transfert pourrait tout de même avoir lieu à condition que la personne concernée y ait consenti, que le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou dans son intérêt, que le transfert soit nécessaire pour des motifs importants d'intérêt général, à la constatation et l'exercice d'un droit en justice, à la sauvegarde des intérêts vitaux de la personne ou d'une autre personne, ou si le transfert intervient au départ d'un registre public qui est ouvert la consultation du public ou de toute personne justifiant d'un intérêt légitime. Le transfert pourrait également être effectué s'il est nécessaire à un intérêt légitime du responsable du traitement et que le responsable du traitement a évalué les conséquences relatives à un transfert de données.

Ce dernier élément apparaît très problématique.

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, des modifications devraient être apportées 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.

CONCLUSION

En conclusion, il conviendrait d'adopter une proposition de résolution. L'Assemblée nationale se féliciterait 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. La proposition de résolution souligne également le renforcement des règles de recueil du consentement et l'augmentation conséquente des sanctions financières en cas de non-respect des dispositions légale.

Cependant, si toutes ces dispositions sont à saluer, il n'en demeure pas moins que d'autres éléments sont aujourd'hui particulièrement inquiétants et porteurs de conséquences politiques, économiques et juridiques considérables, contre lesquelles l'Assemblée nationale doit se prononcer.

Aussi est-il indispensable que les autorités nationales de protection conservent toutes leurs compétences dès lors qu'un traitement cible spécifiquement les résidents de leur pays, quel que soit le territoire sur lequel se situe l'établissement principal de ce responsable de traitement. Il est également nécessaire 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 *a priori* et d'autorisation des autorités. De même, 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 très clairement 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 ne constituent pas seulement un enjeu économique dont il conviendrait d'optimiser la rentabilité. Leur protection et l'encadrement de leur traitement sont avant tout un enjeu en termes de libertés individuelles.

Un engagement de la représentation nationale sur cette question constituerait un message politique fort adressé aux résidents 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.

Il faut enfin souligner que la Commission européenne veut avancer très vite sur ce texte que l'on évoque même une adoption définitive dès 2013.

TRAVAUX DE LA COMMISSION

La Commission s'est réunie le 7 février 2012, sous la présidence de M. Pierre Lequiller, Président, pour examiner le présent rapport.

« **M. Philippe Gosselin, rapporteur**. La proposition de résolution que j'ai déposée comporte quelques différences avec celle de notre collègue Patrick Bloche, mais je ne suis pas en opposition avec ce qui vient d'être dit, bien entendu. Nos positions sont très proches. Je n'avais pas non plus été insensible aux travaux menés par la mission d'information sur la révolution numérique, que j'avais suivis avec beaucoup d'intérêt. 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 Etats 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 depuis l'adoption de la directive en 1995. Les données personnelles des citoyens ne sont plus seulement contenues dans des fichiers mis en place par les Etats ou les administrations, mais sont désormais traitées par différents acteurs publics et privés.

A 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, à l'informatique en nuage (« *cloud coumputing* ») 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 européen 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 et a très récemment, le 25 janvier 2012, proposé une proposition de règlement pour l'ensemble des matières relevant de la directive de 1995, les questions relevant de l'ancien troisième pilier (coopération policière et judiciaire en matière pénale) faisant l'objet d'une proposition de directive.

L'Union européenne est donc à un moment charnière de sa politique de protection de la vie privée des résidents 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 et résidents européens.

L'entrée en vigueur du traité de Lisbonne, le 1er décembre 2010, a donné force contraignante à la Charte des droits fondamentaux, qui dispose en son article 8 que toute personne a droit à la protection des données à caractère personnel la concernant. Par ailleurs, le nouvel article 16 du traité sur le fonctionnement de l'Union européenne définit les règles d'adoption des textes européens permettant de garantir le droit à la protection des données personnelles.

Cette proposition est porteuse de nombreuses avancées, attendues et nécessaires. Ainsi, les citoyens se verraient reconnaître un droit à l'oubli numérique, les règles de recueil de leur consentement seraient renforcées, les correspondants informatiques et libertés seraient rendus obligatoires dans les administrations publiques et certaines entreprises, ces dernières devraient 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 seraient considérablement renforcées, *etc*. 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.

Afin d'assurer une réelle harmonisation des droits nationaux ainsi qu'une protection uniforme des droits à la vie privée et à la protection des données dans l'Union, la Commission européenne propose de réformer la directive de 1995 par un règlement, qui sera donc d'application directe et ne nécessitera pas de transposition. Un règlement est également jugé nécessaire aux acteurs économiques afin de garantir la sécurité juridique, la transparence des règles et de limiter les entraves au marché intérieur.

Le caractère massif des échanges de données à caractère personnel, l'internationalisation de ces échanges, la marchandisation des données personnelles et l'attrait commercial que suscitent les informations nominatives, les nouvelles possibilités technologiques qui permettent d'accroître les capacités de stockage et de conservation des données dans des proportions auparavant

inimaginables sont autant d'éléments qui ont fait naître la revendication d'un droit à l'oubli.

Le rapporteur estime que la mise en œuvre d'un droit général à l'oubli pourrait bien se révéler impraticable. Il souhaiterait que, dans un souci de réalisme, le droit à l'oubli soit en priorité imposé aux réseaux sociaux, car ces derniers ont fait naître ces dernières années des problématiques très spécifiques en termes de protection des données personnelles. La Commission européenne propose aussi d'instituer le droit à la portabilité des données.

Il appartiendrait au responsable du traitement de prendre les mesures techniques et organisationnelles appropriées, tant au moment de la conception que de l'exécution du traitement. Les principes de la protection des données dès la conception (« *privacy by design* ») et de la protection des données par défaut seraient posés. Une obligation de notification des violations des données personnelles, non seulement à l'autorité de contrôle, mais aussi aux personnes concernées, serait instituée pour tous les responsables de traitement. Les sanctions contre les entreprises pourraient atteindre, dans les cas les plus graves, au maximum, 2 % du chiffre d'affaires mondial.

J'estime que l'introduction du critère de l'établissement principal du responsable de traitement pour déterminer l'autorité compétente aura des conséquences politiques et économiques considérables. Nous partageons cette préoccupation avec Patrick Bloche.

Ainsi, pour un responsable de traitement installé dans plusieurs Etats 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 conséquentes politiques importantes, puisqu'elle participera à un éloignement sensible des citoyens des autorités compétentes. Comment les résidents français pourront-ils en effet comprendre, et accepter, qu'une entreprise installée sur le territoire français, traitant des données personnelles de résidents 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 plutôt 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 Etat membre.

De plus, cette image technocratique sera également renforcée par le mécanisme de coopération et d'assistance mutuelle entre autorités européennes, tel qu'il est 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 résidents d'autres Etats membres soit portée à la connaissance des autres autorités impactées. Il en est de même, en cas de consultation de l'autorité de l'établissement principal sur des traitements à risques, tels que les traitements biométriques, déployés dans toute l'Europe. Quand bien même le règlement serait un instrument permettant une plus grande harmonisation, le risque de « *forum shopping* » n'en serait pas moins réel : en effet, la disparité de la mise en œuvre de la protection des données personnelles en Europe découle au moins autant des différences existant entre le droit des Etats membres que des différences d'approche retenues par les autorités de protection nationales, certaines se montrant particulièrement souples.

Au-delà des conséquences évoquées ci-dessus liées à l'introduction du critère de l'établissement principal dans le texte, cette réforme aboutirait 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 européenne 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. Le recours à la « comitologie » est excessif.

Enfin, les transferts vers les Etats tiers ne seraient pas suffisamment encadrés, notamment avec la nouvelle possibilité d'auto-évaluation par les responsables du traitement eux-mêmes.

Je souhaiterais enfin, compte tenu des travaux menés depuis le dépôt de la proposition de résolution, proposer trois amendements à la PPRE :

- au point 6, ajouter la préoccupation suivante :

« Il conviendra toutefois de s'assurer que ce droit permette aux personnes concernées d'obtenir la suppression de données mises en ligne par un tiers » ;

- au point 9, rédiger ainsi, afin de faire apparaître les préoccupations sur la situation des salariés délégués à la protection des données et sur le caractère obligatoire de la désignation, qui pourrait être contre-productif :

« 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 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. 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. »

- amendements de correction rédactionnelle et de précision aux paragraphes 7 et 8, ainsi qu'aux points 6, 8, 9, 12 et 14 de la proposition de résolution.

En conclusion, il conviendrait d'adopter une proposition de résolution, soulignant que l'Assemblée nationale se félicite 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. La proposition de résolution met également en lumière le renforcement des règles de recueil du consentement et l'augmentation conséquente des sanctions financières en cas de non-respect des dispositions légale.

Cependant, si toutes ces dispositions sont à saluer, il n'en demeure pas moins que d'autres éléments sont aujourd'hui particulièrement inquiétants et porteurs de conséquences politiques, économiques et juridiques considérables, contre lesquelles l'Assemblée nationale doit se prononcer. Notre droit d'alerte doit s'exercer avant qu'il ne soit trop tard. »

L'exposé du rapporteur a été suivi d'un débat, commun à l'examen de ce rapport et de celui de M. Patrick Bloche sur sa proposition de résolution européenne n° 4195 relative à 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.

« **Le Président Pierre Lequiller.** Je remercie les rapporteurs pour la qualité de leurs exposés.

M. Guy Geoffroy. Les rapports de nos collègues sont très éclairants. Le chantier sur lequel s'est engagée la Commission européenne constitue un enjeu majeur. Le traitement et la protection des données personnelles sont au cœur de nos préoccupations et j'ai eu souvent à traiter du sujet pour la commission des affaires européennes, notamment sous l'angle du traitement des données des dossiers passagers (PNR).

Ce projet de règlement concerne l'encadrement des traitements de données personnelles qui relevaient auparavant de l'ancien premier pilier. Dans la mesure où il s'agit d'un règlement qui sera d'application directe, il n'y aura pas de transposition, comme c'est le cas lorsqu'une directive est mise en œuvre par les Etats membres. Tout se joue donc maintenant.

C'est pourquoi, je voudrais souligner que si ce texte comporte des avancées bien réelles, certains points sont à combattre avec vigueur.

Ainsi, la possibilité, pour les Etats membres, d'établir leur compétence lorsque les utilisateurs visés sont des résidents européens, même si le lieu d'implantation de l'entreprise est extra-européen est un point très positif. La reconnaissance de nouveaux droits comme le droit à l'oubli et à la portabilité va également dans le bon sens.

Par contre, le critère de l'établissement principal, selon lequel le droit national applicable à tous les traitements de données effectués par une entreprise serait celui de l'Etat membre dans lequel l'établissement principal de l'entreprise est implanté, est inacceptable. Il porte un réel risque de dérive vers le moins-disant, ce qui serait très préjudiciable aux droits des particuliers alors que la Commission européenne fait de la défense des droits des citoyens, une priorité. Ce point doit donc être vivement combattu.

Enfin, il convient de souligner que la réforme présentée par la Commission européenne comprend également un volet relatif à la coopération policière et judiciaire pénale. La refonte de la décision cadre de 2008 applicable à la protection des données en matière de coopération policière et judiciaire pénale, sur laquelle je serai amené à présenter une communication prochainement, constitue également un enjeu majeur en termes de protection des données. La modification du champ d'application de la décision-cadre, qui ne s'applique qu'aux échanges de données entre Etats membres, et le renforcement des droits des personnes concernées, seront au cœur des négociations.

M^me^ Corinne Erhel. Je voudrais aussi remercier les rapporteurs et excuser François Brottes qui est aussi à l'initiative de la proposition de résolution présentée par M. Patrick Bloche.

On assiste à l'explosion des réseaux sociaux. Derrière cette réussite médiatisée, se trouvent des internautes qui plébiscitent de nombreuses applications qui permettent de publier, sur ces réseaux sociaux, leurs opinions, leurs lectures, leurs déplacements. L'ampleur de ces réseaux est telle qu'ils sont devenus une composante importante de la croissance de nos économies. Leur succès est basé sur leur gratuité, l'audience des sites assurant des revenus publicitaires à leurs éditeurs qui sont de plus en plus en mesure de proposer aux annonceurs des campagnes ciblées grâce aux données dont ils disposent. Les données personnelles peuvent donc être considérées comme l'or noir de l'économie numérique. Face à ce phénomène, il est devenu nécessaire de renforcer l'information et la maîtrise des utilisateurs sur leurs données. Les discours critiques sur Internet et les réseaux sociaux sont nombreux mais ils constituent une véritable révolution culturelle qui a permis aux individus de s'exprimer et de s'informer. Néanmoins, cette possibilité leur est offerte par des fournisseurs de services qui s'approprient des données permettant de les identifier, de les localiser et d'en savoir parfois beaucoup trop sur eux. Ce n'est pas parce que les individus s'exposent plus

aisément que nous devons négliger cet aspect fondamental de la protection de l'individu qui est la maîtrise de ses données personnelles. C'est pourquoi le droit à l'oubli sur les réseaux sociaux est un point capital.

L'objectif n'est, ni de pénaliser l'activité des fournisseurs de service, ni de dissuader les utilisateurs d'en faire usage, mais de leur permettre d'user de ces données en toute connaissance de cause et de prévenir des situations contentieuses ou des utilisations malveillantes. Il est nécessaire de fixer des standards élevés de qualité, qui pourront à terme s'imposer comme un élément de différenciation entre les acteurs européens de l'économie numérique. Intégrer la protection des données personnelles dès la conception des services permettrait de distinguer les services respectant ces standards par rapport aux concurrents ne respectant pas de tels critères.

Il faut aussi réserver le stockage des données sensibles aux services de l'informatique en nuages localisés dans l'Union européenne afin d'encourager l'innovation dans ce domaine. La réalisation d'audits de sécurité réguliers est également un point sur lequel nous avons souhaité insister.

Enfin, nous devons considérer spécifiquement le traitement des données relatives aux mineurs, nombreux sur les réseaux sociaux. Ils doivent bénéficier d'une protection renforcée, conformément aux principes de notre droit.

Pour conclure, je rappellerais que les dispositions de la proposition de résolution visent à instaurer une plus grande confiance entre utilisateurs et fournisseurs de service. C'est pourquoi, nous défendons le principe de l'action de groupe et, comme la Commission nationale de l'informatique et des libertés, nous nous opposons à la mise en œuvre, tel que le prévoit le projet, du critère de l'établissement principal afin d'assurer aux citoyens une protection optimale basée sur le principe de proximité.

Le Président Pierre Lequiller. J'aurais souhaité qu'un accord soit possible mais, dans la mesure où cela n'a pas été le cas, je dois mettre aux voix les propositions de résolution.

La proposition de résolution présentée par M. Patrick Bloche est *rejetée*.

M. Philippe Gosselin, rapporteur. Même si nos propositions de résolution sont distinctes, nous essayons d'aller dans le même sens. Il y a bien entendu un vote mais il faut également insister sur nos points communs et je souhaite faire un pas en avant. C'est pourquoi je fais mien le point de la proposition présentée par Patrick Bloche sur l'adoption par les Etats membres de l'Union européenne et les Etats 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 des commissaires à la protection des données et de la vie privée. Je propose de l'intégrer par voie d'amendement.

M. Patrick Bloche, rapporteur. Cet amendement est heureux car, en fait, nos deux propositions ne diffèrent réellement que sur la possibilité d'actions de groupe. Dix-sept ans après la mise en œuvre de la directive de 1995, il est essentiel pour la France de peser dans un domaine où elle a été pionnière avec la loi informatique et libertés. Adopter avant la fin de la législature une telle résolution serait un signal très fort. Rappelons enfin que le règlement sera d'application directe et que ce qui se joue aujourd'hui est déterminant. »

La proposition de résolution présentée par M. Philippe Gosselin, ainsi amendée, dont le texte figure ci-après, *est adoptée.*

La Commission *a* par ailleurs *approuvé* la proposition de règlement (E 7055) sous réserve des observations formulées dans la proposition de résolution. »

ANNEXE :
PROPOSITION DE RESOLUTION
(adoptée par la Commission des affaires européennes)

PROPOSITION DE RESOLUTION EUROPEENNE 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 modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Vu la communication de la Commission européenne au Parlement européen et au Conseil « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » [COM (2010) 609 final],

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/ 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 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 pour 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 Etats 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 Etat sur tout traitement de données ciblant spécifiquement la population de cet Etat, quel que soit l'Etat 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 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 ;

14. Regrette la concentration de pouvoirs considérables entre les mains de la Commission européenne, aux dépends 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 transferts, 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. »