COMMISSION EUROPÉENNE

Bruxelles, le 25.1.2012
COM(2012) 9 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Protection de la vie privée dans un monde en réseau
Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle

(Texte présentant de l'intérêt pour l'EEE)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Protection de la vie privée dans un monde en réseau
Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle

(Texte présentant de l'intérêt pour l'EEE)

1. LES DÉFIS ACTUELS EN MATIÈRE DE PROTECTION DES DONNÉES

La rapidité des évolutions technologiques et la mondialisation modifient en profondeur la façon dont un volume sans cesse croissant de données à caractère personnel est collecté, consulté, utilisé et transféré. De nouveaux modes de partage de l'information via les réseaux sociaux et de stockage à distance de grandes quantités de données sont entrés dans les habitudes de nombre des 250 millions d'internautes en Europe. Parallèlement, les données à caractère personnel sont devenues un atout pour de nombreuses entreprises. La collecte, la globalisation et l'analyse de données concernant des clients potentiels représentent souvent une part importante de leurs activités économiques[1].

Dans ce nouvel environnement numérique, **les personnes physiques ont le droit d'exercer une maîtrise effective sur leurs données**. En Europe, la protection des données est un droit fondamental qui est consacré à l'article 8 de la charte des droits fondamentaux de l'Union européenne ainsi qu'à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE), et qui doit être protégé en conséquence.

S'ils n'ont pas confiance, les consommateurs hésiteront à effectuer des achats en ligne et à recourir à de nouveaux services. Dès lors, il est également impératif de garantir un niveau élevé de protection des données pour accroître la confiance des consommateurs dans les services en ligne et réaliser le potentiel de l'économie numérique, ce qui stimulera **la croissance économique et la compétitivité des entreprises de l'Union**.

Des règles cohérentes et modernes applicables dans l'ensemble de l'UE s'imposent pour permettre la libre circulation des flux de données d'un État 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. Une telle évolution est essentielle pour que le marché unique fonctionne sans heurts, **stimule**

[1] Le marché de l'analyse de grands ensembles de données enregistre une croissance mondiale annuelle de 40 %: http://www.mckinsey.com/mgi/publications/big_data/.

la croissance économique, crée de nouveaux emplois et encourage l'innovation[2]. Une modernisation des règles de l'UE relatives à la protection des données, qui renforce la dimension «marché intérieur» de ces dispositions, garantit aux personnes physiques un niveau élevé de protection des données et crée des conditions propices à la sécurité juridique, à la clarté et à la cohérence; elle joue par conséquent un rôle crucial dans le plan d'action de la Commission européenne mettant en œuvre le programme de Stockholm[3] et dans la stratégie numérique pour l'Europe[4]; plus largement, elle contribue à la stratégie de croissance de l'Union (stratégie Europe 2020)[5].

La directive[6] de l'Union de 1995, instrument législatif principal de la protection des données à caractère personnel en Europe, a posé un jalon dans l'histoire de la protection des données. Ses objectifs, qui consistent à assurer le fonctionnement du marché unique et la protection effective des libertés et droits fondamentaux des personnes physiques, demeurent d'actualité. Mais elle a été adoptée il y a 17 ans, à une époque où l'internet n'en était qu'à ses premiers balbutiements. Dans le nouvel environnement numérique qui s'est créé, avec ses défis, les règles en vigueur ne présentent ni le degré d'harmonisation requis ni l'efficacité nécessaire pour garantir le droit à la protection des données à caractère personnel. C'est pourquoi la Commission européenne propose de réformer fondamentalement le cadre de la protection des données dans l'Union.

Le traité de Lisbonne a en outre introduit, à l'article 16 du TFUE, une base juridique nouvelle en vue d'une approche modernisée et globale de la protection des données et de la libre circulation des données à caractère personnel, qui couvre également la coopération policière et judiciaire en matière pénale[7]. Cette approche s'est traduite dans les communications de la Commission européenne relatives au programme de Stockholm et au plan d'action le mettant en œuvre[8], qui insistent sur la nécessité pour l'Union de «se doter d'un régime complet de protection des données personnelles couvrant l'ensemble des compétences de l'Union» et de «veiller à ce que le droit fondamental à la protection des données soit appliqué systématiquement».

Afin de préparer en toute transparence la réforme du cadre de l'Union relatif à la protection des données, la Commission a organisé, depuis 2009, des consultations publiques sur la question[9]; elle a également noué un dialogue étroit avec les parties

---

2 Voir également les conclusions du Conseil européen du 23 octobre 2011 qui ont souligné le «rôle majeur» du marché unique «dans la croissance et l'emploi» et insisté sur la nécessité d'achever le marché unique numérique d'ici 2015.

3 COM(2010) 171 final.

4 COM(2010) 245 final.

5 COM(2010) 2020 final.

6 Directive 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, JO L 281 du 23.11.1995, p. 31.

7 Des règles spéciales relatives aux traitements par les États membres dans le domaine de la politique étrangère et de sécurité commune sont fixées par une décision du Conseil fondée sur l'article 39 du TUE.

8 Voir, respectivement, COM(2009) 262 et COM(2010) 171.

9 La réforme de la protection des données a donné lieu à deux consultations publiques: la première a été organisée de juillet à décembre 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) et la seconde, de novembre 2010 à janvier 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

prenantes[10]. Le 4 novembre 2010, la Commission a publié une communication relative à une approche globale de la protection des données à caractère personnel dans l'Union européenne[11] qui exposait les thèmes principaux de la réforme. Entre les mois de septembre et de décembre 2011, la Commission a, en outre, pris part à un dialogue renforcé avec les autorités nationales chargées de la protection des données en Europe, d'une part, et avec le contrôleur européen de la protection des données, d'autre part, afin d'étudier les possibilités d'assurer une application plus cohérente des règles de l'Union relatives à la protection des données dans l'ensemble des États membres[12].

Ces échanges ont fait clairement apparaître que les citoyens comme les entreprises souhaitaient voir la Commission européenne procéder à une réforme globale des règles de l'Union sur la protection des données. Après avoir évalué les conséquences des différentes options politiques envisagées[13], la Commission européenne propose à présent **un cadre législatif solide et cohérent qui transcende les politiques de l'Union, renforce les droits des personnes physiques, consolide la dimension «marché unique» de la protection des données et réduit les charges administratives pesant sur les entreprises**[14]. Dans la proposition de la Commission, le nouveau cadre serait constitué par:

– un **règlement** (qui remplace la directive 95/46/CE) instituant un cadre général de l'UE en matière de protection des données[15];

– et une **directive** (qui remplace la décision-cadre 2008/977/JAI[16]) énonçant des règles relatives à la protection des données à caractère personnel traitées à des fins de **prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes.**

---

10 Des consultations ciblées ont été organisées en 2010 avec les États membres et des parties prenantes du secteur privé. Au mois de novembre 2010, la commissaire européenne chargée de la justice, Mme Viviane Reding, a organisé une table ronde sur la réforme de la protection des données. Durant toute l'année 2011 se sont également tenus des ateliers et des séminaires consacrés à des questions précises (telles que les notifications des violations de données).

11 COM(2010) 609.

12 Voir la lettre de M[me] Viviane Reding, commissaire européenne chargée de la justice, adressée le 19 septembre 2011 aux membres du groupe de travail «Article 29», publiée à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Voir l'analyse d'impact SEC(2012) 72.

14 La réforme comportera ultérieurement des modifications destinées à harmoniser des instruments spéciaux et sectoriels tels que le règlement (CE) n° 45/2001, JO L 8 du 12.1.2011, p. 1.

15 Le règlement apporte également un petit nombre d'adaptations techniques à la directive «vie privée et communications électroniques» (directive 2002/58/CE, modifiée en dernier lieu par la directive 2009/136/CE, JO L 337 du 18.12.2009, p. 11) pour tenir compte de la transformation de la directive 95/46/CE en règlement. Les conséquences juridiques de fond que le nouveau règlement et la nouvelle directive entraîneront pour la directive «vie privée et communications électroniques» feront, le moment venu, l'objet d'un examen par la Commission qui tiendra compte de l'issue des négociations menées sur les propositions actuelles avec le Parlement européen et le Conseil.

16 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, JO L 350 du 30.12.2008, p. 60. Un rapport sur la transposition de la décision-cadre par les États membres [COM(2012) 12] figure dans le train de mesures réformant la protection des données.

La présente communication expose les éléments principaux de la réforme du cadre de l'UE relatif à la protection des données.

2. PERMETTRE AUX PERSONNES PHYSIQUES DE MAÎTRISER LES DONNÉES LES CONCERNANT

La directive 95/46/CE, principal acte législatif de l'UE en vigueur en matière de protection des données, n'harmonise pas suffisamment, dans les États membres, les modalités d'exercice, par les personnes physiques, du droit à la protection des données. Les pouvoirs conférés aux autorités nationales chargées de la protection des données ne sont pas non plus suffisamment harmonisés pour garantir l'application cohérente et effective des règles en la matière. Aussi, exercer ces droits est-il, dans la pratique, plus difficile dans certains États membres que dans d'autres, surtout dans l'environnement en ligne.

Ces difficultés sont également dues à l'importance du volume des données collectées chaque jour et au fait que souvent, les utilisateurs n'ont pas pleinement conscience que des données les concernant sont collectées. Bien que de nombreux Européens considèrent que la communication de données à caractère personnel est un phénomène de plus en plus fréquent aujourd'hui[17], 72 % des internautes en Europe sont encore préoccupés par le fait qu'il leur soit demandé de communiquer en ligne trop de données les concernant[18]. Ils ont le sentiment de ne pas avoir la maîtrise des données qui les concernent. Ils ne sont pas correctement informés du sort réservé à ce type de données, de l'identité du destinataire et de la finalité de leur transmission. Ils ignorent souvent les modalités d'exercice de leurs droits dans l'environnement en ligne.

«Droit à l'oubli numérique»

Un étudiant européen, membre d'un réseau social en ligne, décide de demander l'accès à toutes les données qui le concernent et que ce réseau détient. À cette occasion, il se rend compte que ce réseau social collecte beaucoup plus de données que ce qu'il imaginait, et que certaines données à caractère personnel dont il pensait qu'elles avaient été effacées étaient toujours conservées.

La réforme des dispositions de l'UE sur la protection des données fera en sorte qu'un tel scénario ne soit plus possible, en introduisant:

- une obligation explicite imposant aux réseaux sociaux en ligne (et à tous les autres responsables du traitement de données) de limiter au minimum le volume des données à caractère personnel qu'ils collectent et qu'ils traitent pour chaque utilisateur;

- une obligation de configurer par défaut le système d'une façon qui garantit que les données ne sont pas rendues publiques;

- une obligation expresse incombant aux responsables du traitement d'effacer les données concernant une personne physique si cette dernière en a explicitement demandé l'effacement et lorsqu'aucun autre motif légitime ne justifie de les conserver.

[17] Voir Eurobaromètre spécial 359 - *Attitudes on Data Protection and Electronic Identity in the European Union*, juin 2011, p. 23.

[18] Ibidem, p. 54.

Dans ce cas particulier, le fournisseur du réseau social serait ainsi tenu d'effacer immédiatement et complètement les données concernant cet étudiant.

Ainsi que la Commission l'a mis en évidence dans la stratégie numérique pour l'Europe, les préoccupations quant au respect de la vie privée figurent parmi les raisons les plus fréquentes pour lesquelles les consommateurs s'abstiennent d'acheter des produits et des services en ligne. Vu la contribution du secteur des technologies de l'information et des communications (TIC) à l'augmentation globale de la productivité en Europe, due pour 20 % directement au secteur des TIC et pour 30 % aux investissements réalisés dans les TIC[19], la confiance dans les services de cette nature est essentielle pour stimuler la croissance de l'économie dans l'Union européenne et la compétitivité de son industrie.

Notification des violations de données

Des pirates informatiques ont pris pour cible un service de jeux qui s'adresse à des clients établis sur le territoire de l'UE. La violation a touché des bases de données contenant des informations à caractère personnel (dont les noms et adresses, voire les numéros de carte de crédit) de dizaines de millions de clients dans le monde entier. La société prestataire a attendu une semaine avant d'en avertir les clients concernés.

Grâce à la réforme des dispositions de l'UE sur la protection des données, un tel incident ne pourra plus se produire: Les nouvelles dispositions obligeront les sociétés:

- à renforcer leurs dispositifs de sécurité pour prévenir et éviter les violations de données;

- à notifier sans retard indu les violations de données tant à l'autorité nationale chargée de la protection des données – si possible, dans les 24 heures suivant la découverte de la violation – qu'aux personnes physiques concernées.

Les nouvelles propositions législatives présentées par la Commission visent à renforcer les droits des personnes physiques, à les doter de moyens efficaces et opérationnels pour garantir qu'elles aient pleinement connaissance du sort réservé aux données les concernant, et à leur permettre d'exercer leurs droits de façon plus effective.

En vue de renforcer le droit des personnes physiques à la protection des données, la Commission propose de nouvelles règles qui:

permettront aux personnes physiques de mieux maîtriser les données les concernant:

- en faisant en sorte que, lorsque leur **consentement** est exigé, celui-ci soit **explicitement formulé, c'est-à-dire qu'il repose soit sur une déclaration, soit sur un acte non équivoque de l'intéressé**, et qu'il soit donné librement;

- en dotant les internautes d'un **droit** effectif **à l'oubli numérique** dans l'environnement en ligne, c'est-à-dire le droit de faire effacer les données les concernant s'ils retirent leur consentement et si aucun autre motif légitime ne justifie la conservation de celles-ci;

[19] Voir Une stratégie numérique pour l'Europe, précitée, p. 4.

- en leur garantissant un accès aisé à leurs propres données et un **droit à la portabilité de celles-ci**: c'est-à-dire le droit d'obtenir du responsable du traitement une copie des données conservées et la liberté de les transférer d'un prestataire de services à un autre, sans entrave;

- en renforçant **le droit à l'information**, afin que chacun comprenne pleinement le mode de traitement des données les concernant, en particulier lorsque ces traitements concernent les **enfants**;

améliorera les moyens dont disposent les personnes physiques pour exercer leurs droits:

- en renforçant l'**indépendance et les pouvoirs des autorités nationales chargées de la protection des données,** de manière à ce qu'elles soient à même de traiter les réclamations de manière effective en ayant le pouvoir de mener des enquêtes efficaces, de prendre des décisions contraignantes et d'imposer des sanctions effectives et dissuasives;

- en améliorant les possibilités de former des **recours administratifs et juridictionnels** en cas de **violation** des droits relatifs à la protection des données. En particulier, les associations qui satisfont à certaines conditions pourront saisir les tribunaux au nom de la personne physique concernée;

renforceront la sécurité des données:

- en encourageant l'utilisation de **technologies renforçant la protection de la vie privée** (c'est-à-dire de technologies *qui protègent la confidentialité des informations en réduisant au minimum la conservation de données à caractère personnel*), d'un **paramétrage par défaut respectueux de la vie privée** et de **régimes de certification du respect de la vie privée**;

- en introduisant **une obligation générale**[20] imposant aux responsables du traitement **de notifier sans retard indu les violations de données** tant aux autorités chargées de la protection de celles-ci (si possible dans un délai de 24 heures) qu'aux personnes physiques concernées;

accroîtront la responsabilité des personnes traitant les données, notamment:

- en exigeant des responsables du traitement dans les sociétés employant plus de 250 salariés et dans celles qui interviennent dans les traitements à risques qui, du fait de leur nature, de leur portée ou de leur finalité, présentent des risques particuliers au regard des droits et libertés des personnes physiques («traitements à risques»), qu'ils désignent un **délégué à la protection des données**;

- en introduisant le **principe de «protection des données dès la conception»** pour faire en sorte que les garanties en matière de protection des données soient prises en considération dès la phase de planification des procédures et des systèmes de traitement;

[20] Une telle obligation n'existe actuellement que dans le secteur des télécommunications en vertu de la directive «vie privée et communications électroniques».

- en introduisant l'obligation, pour les organisations associées à des traitements à risques, d'effectuer des **analyses d'impact relatives à la protection des données**.

3. DES RÈGLES DE PROTECTION DES DONNÉES ADAPTÉES AU MARCHÉ UNIQUE NUMÉRIQUE

Bien que la directive en vigueur vise à garantir un niveau équivalent de protection des données dans l'ensemble de l'UE, les règles adoptées par les États membres divergent encore considérablement. Il n'est dès lors pas exclu que les responsables du traitement doivent composer avec 27 législations nationales prévoyant des obligations différentes. Il s'ensuit une **fragmentation de l'environnement juridique** qui a engendré une **insécurité juridique** et une protection inégale des personnes physiques. Cette situation génère des **coûts et des charges administratives inutiles** qui pèsent sur les entreprises et constitue un frein pour celles qui sont présentes sur le marché unique et qui souhaiteraient étendre leurs activités à d'autres États membres.

Les ressources et les pouvoirs dont disposent les autorités nationales chargées de la protection des données varient sensiblement d'un État membre à l'autre[21]. Ceci se traduit dans certains cas par l'incapacité de ces autorités à exercer leur mission répressive de manière satisfaisante. La coopération entre ces autorités à l'échelle européenne, au sein du groupe consultatif existant (le «groupe de travail Article 29»)[22], n'aboutit pas toujours à une application cohérente des règles relatives à la protection des données et appelle par conséquent des améliorations.

Application cohérente, dans l'ensemble de l'Europe, des règles relatives à la protection des données

Une entreprise multinationale détenant plusieurs établissements sur le territoire de l'Union a déployé dans toute l'Europe un système de cartographie en ligne qui collecte des images de tous les édifices privés et publics et peut, le cas échéant, photographier des personnes dans la rue. Dans un État membre, l'insertion de photos non floutées de personnes ignorant qu'elles étaient photographiées a été considérée comme illégale, tandis que dans d'autres, cette pratique ne constituait pas une infraction à la législation sur la protection des données. Cette situation n'a pas permis de dégager une position cohérente entre autorités nationales chargées de la protection des données pour remédier au problème.

Grâce à la réforme des règles de l'UE sur la protection des données, ce cas de figure ne pourra plus se présenter à l'avenir, parce que:

- les exigences et garanties en matière de protection des données seront énoncées dans un règlement de l'Union directement applicable dans l'ensemble du territoire de celle-ci;

- seule l'autorité chargée de la protection des données dans l'État membre où la société a son établissement principal sera compétente pour se prononcer sur la légalité du comportement de celle-ci;

---

21 Pour de plus amples informations à cet égard, voir l'analyse d'impact accompagnant les propositions législatives, SEC(2012) 72.

22 Le groupe de travail «Article 29» a été institué en 1996 (par l'article 29 de la directive 95/46/CE); il a un caractère consultatif et se compose de représentants des autorités de contrôle de la protection des données, du Contrôleur européen de la protection des données (CEPD) et de la Commission. Pour de plus amples informations sur ses activités, voir http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

- la coordination rapide et efficace entre autorités nationales chargées de la protection des données, le service étant proposé à des personnes physiques dans plusieurs États membres, contribuera à garantir une application et un respect cohérents des nouvelles règles de l'UE relatives à la protection des données dans l'ensemble des États membres.

Il convient de mieux armer les autorités nationales et de renforcer leur coopération pour garantir la mise en œuvre cohérente et, en définitive, l'application uniforme des règles dans l'ensemble de l'UE.

Un cadre législatif solide, clair et uniforme au niveau de l'Union contribuera à libérer le potentiel du marché unique numérique et à promouvoir la croissance économique, l'innovation et la création d'emplois. L'adoption d'un règlement mettra fin à la fragmentation des régimes juridiques entre les 27 États membres et supprimera les obstacles à l'entrée sur le marché, élément qui revêt une importance particulière pour les micro-entreprises ainsi que pour les petites et moyennes entreprises.

Grâce aux nouvelles dispositions, les sociétés établies dans l'Union bénéficieront en outre d'un avantage dans la concurrence mondiale. Le cadre réglementaire réformé leur permettra en effet de donner à leurs clients l'assurance qu'elles traiteront avec la diligence et le soin requis toute information importante à caractère personnel. La confiance dans un régime réglementaire cohérent institué par l'UE constituera un atout majeur pour les prestataires de services et une incitation pour les investisseurs qui sont à l'affût de conditions optimales lorsqu'ils choisissent un site pour implanter leurs services.

Afin d'accroître la **dimension «marché intérieur» de la protection des données**, la Commission propose:

- d'établir, au niveau de l'UE, des règles relatives à la protection des données au moyen d'un **règlement directement applicable dans tous les États membres**[23] qui mettra fin à l'application cumulative et simultanée de législations nationales différentes en la matière. Cela représentera pour les entreprises une **économie annuelle** nette **d'environ 2,3 milliards d'euros uniquement en charges administratives**;

- de **simplifier l'environnement réglementaire en réduisant considérablement les charges administratives** et en supprimant des **formalités** telles que les obligations générales de notification (ce qui permettra de réaliser des économies annuelles nettes de 130 millions d'euros pour les charges administratives uniquement). Compte tenu de leur importance pour la compétitivité de l'économie européenne, une attention particulière est accordée aux besoins spécifiques des micro-entreprises ainsi qu'à ceux des petites et moyennes entreprises;

- d'**accroître davantage l'indépendance et les pouvoirs des autorités nationales chargées de la protection des données** pour leur permettre de mener des enquêtes, d'arrêter des décisions contraignantes et d'infliger des sanctions effectives

[23] La Commission présente également une proposition de directive pour définir les règles applicables au domaine de la coopération policière et de la coopération judiciaire en matière pénale (voir section 4 ci-après) qui offrira aux États membres une plus grande souplesse dans ce domaine particulier.

et dissuasives; la Commission propose également d'obliger les États membres à les doter de **ressources suffisantes** à cette fin;

- **d'instituer un système de «guichet unique» pour la protection des données dans l'UE:** les responsables du traitement dans l'UE n'auront plus qu'**une seule autorité chargée de la protection des données** comme interlocuteur, à savoir celle de l'État membre dans lequel est situé l'établissement principal de la société;

- de créer les conditions propices à une **coopération rapide et efficace entre autorités chargées de la protection des données**, notamment en imposant à chacune l'obligation d'effectuer des enquêtes et des inspections à la demande d'une autre, et de reconnaître mutuellement leurs décisions;

- **de mettre sur pied un mécanisme de contrôle de la cohérence** au niveau de l'Union pour faire en sorte que les décisions des autorités chargées de la protection des données ayant une portée européenne plus large tiennent pleinement compte des avis émis par d'autres autorités concernées et soient entièrement conformes au droit de l'Union;

- d'accroître l'importance du groupe de travail «Article 29» en le transformant en un **comité européen de la protection des données indépendant**, afin de renforcer sa contribution à l'application cohérente de la législation relative à la protection des données et d'offrir une base de coopération solide entre autorités chargées de la protection des données, en y associant le contrôleur européen de la protection des données, et d'intensifier les synergies et l'efficacité en prévoyant que le secrétariat du Comité européen de la protection des données sera assuré par le Contrôleur européen de la protection des données.

Le nouveau règlement garantira une sauvegarde solide du droit fondamental à la protection des données dans l'ensemble de l'Union européenne et améliorera le fonctionnement du marché unique. Parallèlement - compte tenu du fait, souligné par la Cour de justice de l'Union européenne[24], que le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société[25] et qu'il doit être mis en balance avec d'autres droits fondamentaux conformément au principe de proportionnalité[26] -, le nouveau règlement comprendra des dispositions expresses qui garantiront le respect d'autres droits fondamentaux tels que la liberté d'expression et d'information, le droit de se défendre ainsi que le droit au secret professionnel (notamment pour les professions juridiques) sans porter atteinte au statut des églises tel qu'il est défini dans les législations nationales.

---

24 Arrêt de la Cour de justice de l'Union européenne du 9 novembre 2010 dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke et Eifert, Recueil 2010, non encore publié au Recueil.

25 Conformément à l'article 52, paragraphe 1, de la charte des droits fondamentaux, des limitations peuvent être apportées à l'exercice du droit à la protection des données, à condition que lesdites limitations soient prévues par la loi, respectent le contenu essentiel du droit et des libertés en cause et, dans le respect du principe de proportionnalité, soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

26 Arrêts de la Cour de justice de l'Union européenne du 6 novembre 2003 dans l'affaire C-101/01, Lindqvist, Recueil 2003, p. I-12971, points 82 à 90, et du 16 décembre 2008 dans l'affaire C-73/07, Satamedia, Recueil 2008, p. I-9831, points 50 à 62.

4. L'UTILISATION DE DONNÉES DANS LA COOPÉRATION EN MATIÈRE DE POLICE ET DE JUSTICE PÉNALE

L'entrée en vigueur du traité de Lisbonne et, notamment, la l'introduction d'une nouvelle base juridique (l'article 16 du TFUE) permettent à l'Union d'instaurer un cadre global pour la protection des données qui garantit un niveau élevé de protection des données à caractère personnel tout en respectant les spécificités du domaine de la coopération policière et judiciaire en matière pénale. Le cadre révisé de l'UE relatif à la protection des données peut notamment s'appliquer aux traitements aussi bien transfrontières que nationaux de données à caractère personnel. Les différences existant entre les législations nationales pourraient ainsi être atténuées, au bénéfice probable de la protection des données à caractère personnel considérée dans son ensemble. Cette nouvelle donne pourrait également contribuer à faciliter l'échange d'informations entre les autorités policières et judiciaires nationales et, de ce fait, améliorer la coopération dans la lutte contre les formes graves de criminalité en Europe. À l'heure actuelle, le traitement de données par les autorités policières et judiciaires en matière pénale est essentiellement régi par la décision-cadre 2008/977/JAI, antérieure à l'entrée en vigueur du traité de Lisbonne. La Commission n'a pas le pouvoir d'en faire respecter les dispositions, car il s'agit d'une décision-cadre, ce qui a contribué au caractère disparate de sa transposition. Le champ d'application de la décision-cadre est en outre limité aux traitements à caractère transfrontière[27]. En d'autres termes, le traitement de données à caractère personnel qui n'ont pas été échangées ne relève pas, à l'heure actuelle, des dispositions de l'UE qui régissent ce type de traitement et protègent le droit fondamental à la protection des données. Il en résulte aussi, dans certains cas, des difficultés pratiques pour la police et d'autres autorités, qui peuvent avoir du mal à déterminer le caractère purement national ou transfrontière d'un traitement de données, ou à deviner si des données «nationales» sont susceptibles de faire l'objet d'un échange transfrontière ultérieur[28].

Le nouveau cadre réformé de l'UE relatif à la protection des données vise dès lors à garantir un niveau élevé et cohérent de protection des données afin de **renforcer la confiance mutuelle entre les autorités policières et judiciaires d'États membres différents, facilitant ainsi la libre circulation des données, ainsi que l'efficacité de la coopération entre ces mêmes autorités**.

Pour garantir un niveau élevé de protection des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale et faciliter les échanges de ces données entre les autorités policières et judiciaires nationales, la Commission propose, parmi les mesures prévues dans le train de réformes, une directive qui:

---

27 Plus précisément, la décision-cadre s'applique aux données à caractère personnel qui sont ou ont été transmises ou mises à disposition entre les États membres ou échangées entre des États membres et des institutions, organes et organismes de l'Union (voir article 1er, paragraphe 2).

28 Certains États membres l'ont confirmé dans leurs réponses au questionnaire de la Commission relatif au rapport sur la transposition de la décision-cadre [COM(2012) 12].

- **appliquera les principes généraux en matière de protection des données** à la coopération policière et à la coopération judiciaire en matière pénale, tout en respectant les spécificités de ces domaines[29];

- prévoira des **conditions et critères harmonisés a minima relatifs à d'éventuelles limitations** apportées aux règles générales. Il s'agit notamment du droit des personnes physiques d'être informées lorsque les autorités policières ou judiciaires traitent ou consultent des données les concernant. Ces limitations sont nécessaires pour garantir l'efficacité de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière;

- instaurera **un régime spécial pour prendre en considération la nature particulière des activités répressives**, **notamment une distinction entre diverses catégories de personnes concernées par les données** (telles que les témoins et les suspects), dont les droits peuvent être différents.

5. LA PROTECTION DES DONNÉES DANS LE CONTEXTE DE LA MONDIALISATION

Les droits des personnes physiques doivent continuer d'être garantis lorsque des données à caractère personnel sont transférées de l'Union européenne vers des pays tiers, et dès que des prestataires de services établis dans des pays tiers ciblent des personnes physiques dans les États membres et utilisent ou analysent les données qui les concernent. Par conséquent, les normes de l'UE en matière de protection des données doivent s'appliquer quelle que soit la localisation géographique d'une société ou de son service de traitement des données.

Dans le contexte de mondialisation actuel, les données à caractère personnel sont transférées par delà un nombre croissant de frontières virtuelles et géographiques et conservées sur des serveurs situés dans de nombreux pays. Les sociétés sont plus nombreuses à offrir des services d'informatique en nuage, qui permettent à leurs clients de consulter et de stocker des données sur des serveurs distants. Ces éléments plaident en faveur d'une amélioration des mécanismes actuels de transfert de données vers les pays tiers. Il peut s'agir notamment de décisions relatives au caractère adéquat de la protection - c'est-à-dire des décisions certifiant que les normes de protection des données en vigueur dans des pays tiers sont «adéquates» - et de garanties appropriées telles que des clauses contractuelles types ou des règles d'entreprise contraignantes[30], de manière à garantir un niveau élevé de protection des

29 Voir la Déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la conférence intergouvernementale qui a adopté le traité de Lisbonne.

30 On entend par «règles d'entreprise contraignantes» des codes de bonne pratique fondés sur les normes européennes de protection des données et approuvés par au moins une autorité chargée de cette protection, que des entités établissent de leur plein gré et respectent pour garantir un niveau adéquat de protection à des catégories de transferts de données à caractère personnel entre les entreprises d'un même groupe liées par ces règles. Ces règles ne sont pas expressément prévues par la directive 95/46/CE mais se sont créées dans la pratique entre les autorités chargées de la protection des données, avec le soutien du groupe de travail «Article 29».

données dans les traitements internationaux et à faciliter les flux transfrontières de données.

Les règles d'entreprise contraignantes

Un groupe de sociétés doit régulièrement transférer des données à caractère personnel de ses sociétés apparentées établies sur le territoire de l'UE à celles situées dans des pays tiers. Le groupe souhaiterait introduire un ensemble de règles d'entreprise contraignantes (REC) pour se conformer à la législation de l'Union tout en limitant les obligations administratives afférentes à chaque transfert. Dans la pratique, les REC garantissent l'application d'un corps unique de règles dans l'ensemble du groupe au lieu de devoir conclure un contrat interne pour chacun des transferts.

Conformément aux pratiques en vigueur convenues au sein du groupe de travail «Article 29», la reconnaissance du caractère adéquat des garanties prévues par les REC d'une société exige un contrôle approfondi par trois autorités chargées de la protection des données (une autorité «chef de file» et deux autorités «examinatrices»); plusieurs autres autorités peuvent cependant elles aussi formuler des commentaires. Les législations de nombreux États membres subordonnent en outre les transferts régis par des REC à l'obtention d'autorisations nationales supplémentaires, ce qui rend le processus d'adoption de ces REC très lourd, onéreux, long et complexe.

Après la réforme de la protection des données,

- ce processus sera plus simple et davantage rationalisé;

- les REC ne seront plus validées que par une seule autorité chargée de la protection des données, tandis que des mécanismes prévoiront la participation rapide d'autres autorités concernées;

- une fois qu'une REC aura été approuvée par une autorité, elle sera valable dans toute l'UE sans devoir être, de surcroît, autorisée au niveau national.

Pour **relever les défis de la mondialisation**, il est indispensable, notamment pour les entreprises actives à l'échelle mondiale, de créer des outils et des mécanismes souples permettant de garantir concomitamment la protection sans faille des données à caractère personnel. La Commission propose les mesures suivantes:

- des **règles claires** qui définissent les cas dans lesquels le **droit de l'Union est applicable aux responsables du traitement établis dans des pays tiers**, notamment en précisant que, chaque fois que des produits et des services sont proposés à des personnes physiques dans l'UE ou que leur comportement est analysé, les **règles européennes s'appliquent**;

- la Commission européenne adoptera toute **décision relative au caractère adéquat du niveau de protection des données** sur le fondement de critères clairs et explicites, y compris dans le domaine de la coopération policière et de la justice pénale;

- les flux licites de données vers des pays tiers seront facilités par le renforcement et la simplification des **règles relatives aux transferts internationaux** de données vers des pays non couverts par une décision relative au caractère adéquat du niveau de protection, notamment grâce à la rationalisation et à l'extension du recours à des outils tels que les **règles d'entreprise contraignantes**, de sorte que celles-ci puissent être appliquées à des **responsables du traitement** ainsi qu'à l'intérieur de **groupes de sociétés**, ce qui reflètera mieux le nombre croissant de sociétés effectuant des traitements de données, notamment dans le domaine de l'informatique en nuage;

- engager un **dialogue** et, le cas échéant, des **négociations** avec des pays tiers, en particulier les partenaires stratégiques de l'Union et les pays concernés par la politique européenne de voisinage, et les organisations internationales concernées (comme le Conseil de l'Europe, l'Organisation de coopération et de développement économiques, les Nations unies) afin d'œuvrer, à l'échelle mondiale, à l'adoption de **normes de haut niveau et interopérables en matière de protection des données**.

6. CONCLUSION

La réforme de la protection des données vise à mettre sur pied **un cadre global, cohérent, solide et moderne relatif à la protection des données pour l'Union européenne**. Le droit fondamental des personnes physiques à la protection des données en sera renforcé. D'autres droits, tels que la liberté d'expression et d'information, les droits de l'enfant, la liberté d'entreprise, le droit à un procès équitable et la garantie du secret professionnel (pour les professions juridiques, notamment) ainsi que le statut des églises tel qu'il est défini dans les législations nationales, seront respectés.

La réforme profitera en premier lieu aux personnes physiques, en renforçant leurs droits à la protection des données et leur confiance dans l'environnement numérique. Elle simplifiera considérablement, en outre, l'environnement juridique dans lequel évoluent les entreprises et le secteur public. Le développement de l'économie numérique dans l'ensemble du marché unique de l'UE et au-delà devrait en être stimulé, conformément aux objectifs fixés dans la stratégie Europe 2020 et la stratégie numérique pour l'Europe. Enfin, la réforme accroîtra la confiance entre les autorités répressives afin de faciliter les échanges d'information entre elles ainsi que la coopération dans la lutte contre les formes graves de criminalité en Europe, tout en garantissant aux personnes physiques un niveau élevé de protection.

La Commission européenne collaborera étroitement avec le Parlement européen et le Conseil pour assurer la conclusion, d'ici fin 2012, d'un accord sur le nouveau cadre de l'UE relatif à la protection des données. Tout au long de ce processus d'adoption et au-delà, notamment dans le contexte de la transposition et de l'application des nouveaux instruments juridiques, la Commission poursuivra son **dialogue étroit et transparent avec toutes les parties intéressées,** dont des représentants des secteurs privé et public, parmi lesquels figureront des représentants de la police, de la justice, des autorités de réglementation des communications électroniques, d'organisations de la société civile, d'autorités chargées de la protection des données et du monde universitaire, ainsi que des représentants d'agences spécialisées de l'Union telles qu'Eurojust, Europol, l'Agence des droits fondamentaux et l'Agence européenne chargée de la sécurité des réseaux et de l'information.

Dans un contexte d'évolution constante des technologies de l'information et des comportements sociaux, un tel dialogue est de la plus haute importance pour mettre à profit les contributions qui sont nécessaires pour garantir un niveau élevé de protection des données des personnes physiques, la croissance et la compétitivité des entreprises de l'Union, l'efficacité opérationnelle du secteur public (dont celle des services de police et de la justice) et un faible niveau de charges administratives.