

FR

FR

FR



COMMISSION EUROPÉENNE

Bruxelles, le 4.11.2010
COM(2010) 609 final

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

**«Une approche globale de la protection des données à caractère personnel dans l'Union
européenne»**

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

**«Une approche globale de la protection des données à caractère personnel dans l'Union
européenne»**

**1. NOUVEAUX DEFIS EN MATIERE DE PROTECTION DES DONNEES A CARACTERE
PERSONNEL**

La directive sur la protection des données de 1995¹ a posé un jalon dans l'histoire de la protection des données à caractère personnel dans l'Union européenne. Elle consacre deux des plus anciennes et tout aussi importantes ambitions de l'intégration européenne: d'une part, la protection des libertés et droits fondamentaux des personnes, notamment du droit fondamental à la protection des données, et, d'autre part, la réalisation du marché intérieur, en l'occurrence, la libre circulation des données à caractère personnel.

Quinze ans plus tard, ce double objectif est toujours d'actualité, et les principes consacrés dans la directive restent pertinents. **Cependant, l'évolution technologique rapide et la mondialisation modifient en profondeur notre environnement et nous posent de nouveaux défis en matière de protection des données à caractère personnel.**

Aujourd'hui, les technologies permettent à tout un chacun d'échanger aisément des informations sur son comportement et ses préférences et de les rendre publiques et accessibles à l'échelle mondiale comme jamais auparavant. Les sites de socialisation, dont les centaines de millions de membres proviennent du monde entier, constituent sans doute l'exemple le plus manifeste de ce phénomène, sans en être l'unique illustration. L'«informatique en nuage» - c'est-à-dire l'informatique fondée sur l'internet dans le cadre de laquelle des logiciels, des ressources et des informations partagées se trouvent sur des serveurs lointains («dans les nuages») - pourrait également lancer des défis dans le domaine de la protection des données car elle peut signifier, pour le particulier, une perte de contrôle sur les informations potentiellement sensibles qui le concernent, lorsqu'il stocke ses données à l'aide de programmes hébergés sur l'ordinateur de quelqu'un d'autre. Une étude récente a confirmé que les autorités chargées de la protection des données, les organisations professionnelles et les associations de consommateurs s'accordent à penser que les activités en ligne accroissent les risques pour la protection de la vie privée et des données à caractère personnel².

Parallèlement, **les modes de collecte des données à caractère personnel se complexifient et sont moins facilement décelables.** Par exemple, l'utilisation d'outils sophistiqués permet aux entreprises de mieux connaître le comportement des internautes et ainsi de mieux cibler leurs offres. Le recours accru à des procédures permettant la collecte automatique de données, telles que la vente électronique de titres de transport et le télépéage, ou à des dispositifs de

¹ 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 (JO L 281 du 23.11.1995, p. 31).

² Voir l'étude intitulée *Study on the economic benefits of privacy enhancing technologies*, London Economics, juillet 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14.

localisation géographique permet de localiser plus facilement des personnes, du seul fait que celles-ci utilisent un appareil portable. Les pouvoirs publics utilisent aussi de plus en plus les données à caractère personnel et ce à des fins diverses: pour rechercher des personnes lorsqu'une maladie transmissible se déclare, pour prévenir et combattre plus efficacement le terrorisme et la criminalité, pour gérer leur régime de sécurité sociale, leur système fiscal, dans le cadre de leurs applications d'administration en ligne, etc.

Tous ces éléments soulèvent inévitablement la question de savoir si la législation de l'Union européenne en matière de protection des données permet toujours de relever pleinement et efficacement ces défis.

Pour répondre à cette question, la Commission a lancé un réexamen du cadre juridique actuel, à l'occasion d'une conférence à haut niveau organisée en mai 2009, suivie d'une consultation publique clôturée fin 2009³. Plusieurs études ont également été commandées⁴.

Les résultats obtenus confirment que les principes essentiels de la directive sont toujours valables et qu'il convient de préserver sa neutralité sous l'angle technologique. Plusieurs problèmes ont cependant été recensés, dont la résolution exigera de relever des défis spécifiques. Il s'agit notamment de:

- *Tenir compte des répercussions des nouvelles technologies*

Les réponses apportées dans le cadre des consultations, émanant tant de particuliers que d'organisations, confirment la nécessité de clarifier et de préciser l'application des principes de la protection des données aux nouvelles technologies, afin de garantir aux personnes une protection réelle et effective des données à caractère personnel les concernant, quelle que soit la technologie utilisée pour traiter ces données, et que les responsables du traitement des données prennent pleinement conscience des répercussions des nouvelles technologies sur la protection des données. Il a été partiellement répondu à cette nécessité au moyen de la directive 2002/58/CE (dite directive «vie privée et communications électroniques»)⁵, qui spécifie et complète la directive générale relative à la protection des données dans le secteur des communications électroniques⁶.

³ Voir les réponses à la consultation publique organisée par la Commission: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm.

Des consultations plus ciblées des parties concernées ont eu lieu tout au long de l'année 2010. M^{me} Viviane Reding, vice-présidente de la Commission, a également présidé une réunion à haut niveau avec les parties prenantes, qui s'est tenue le 5 octobre 2010 à Bruxelles. Par ailleurs, la Commission a consulté le groupe de travail «Article 29» qui a apporté une contribution détaillée à la consultation de 2009 (document WP 168) et a adopté, en juillet 2010, un avis spécifique sur le principe de la l'«accountability» (document WP 173).

⁴ Outre l'étude sur les avantages économiques des technologies renforçant la protection de la vie privée (citée à la note de bas de page n° 2), voir également l'étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière de l'évolution technologique, janvier 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf). Une étude préparatoire à l'analyse d'impact du futur cadre juridique de l'UE en matière de protection des données est également en cours.

⁵ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

⁶ La directive 95/46/CE sur la protection des données fixe les normes de protection pour l'ensemble des actes législatifs de l'UE, y compris la directive 2002/58/CE («vie privée et communications

- *Renforcer la dimension «marché intérieur» de la protection des données*

L'une des principales préoccupations récurrentes des parties prenantes, et notamment des entreprises multinationales, est l'harmonisation insuffisante des législations des États membres en matière de protection des données, en dépit de l'existence d'un cadre juridique commun de l'UE. Celles-ci ont souligné la nécessité d'accroître la sécurité juridique, d'alléger la charge administrative et d'assurer des conditions égales aux acteurs économiques et autres responsables du traitement.

- *Faire face à la mondialisation et améliorer les transferts internationaux de données*

Plusieurs parties prenantes ont souligné que la sous-traitance accrue du traitement, très souvent en dehors de l'Union, soulève plusieurs problèmes liés au droit applicable au traitement et à l'attribution de la responsabilité y afférente. Quant aux transferts internationaux de données, bon nombre d'organisations ont estimé que les régimes actuels ne sont pas pleinement satisfaisants et doivent être revus et rationalisés de manière à simplifier les transferts et à les rendre moins laborieux.

- *Renforcer le cadre institutionnel en vue de l'application effective des règles de protection des données*

Les parties prenantes s'accordent à penser qu'il convient de renforcer le rôle des autorités chargées de la protection des données afin d'améliorer l'application des règles dans ce domaine. Certaines organisations ont aussi réclamé une plus grande transparence des travaux du groupe de travail «Article 29» (voir la section 2.5 ci-dessous) et une clarification de sa mission et de ses pouvoirs.

- *Améliorer la cohérence du cadre juridique régissant la protection des données*

Pendant la consultation publique, toutes les parties prenantes ont souligné la nécessité de disposer d'un instrument global, applicable aux opérations de traitement des données dans tous les secteurs et tous les domaines d'action de l'Union, garantissant une approche intégrée ainsi qu'une protection sans faille, cohérente et efficace⁷.

Les défis susmentionnés **requièrent que l'Union élabore une approche globale et cohérente, qui garantisse le plein respect du droit fondamental des personnes à la protection des données à caractère personnel, tant dans l'Union qu'en dehors de celle-ci.** Le traité de Lisbonne a doté l'Union de moyens supplémentaires pour relever ces défis: la Charte des droits fondamentaux de l'Union européenne – dont l'article 8 consacre un droit autonome à la protection des données à caractère personnel – est désormais juridiquement

électroniques») (modifiée par la directive 2009/136/CE – JO L 337 du 18.12.2009, p. 11). La directive «vie privée et communications électroniques» s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications. Elle a traduit les principes énoncés dans la directive sur la protection des données en règles spécifiques applicables au secteur des communications électroniques: la directive 95/46/CE s'applique entre autres aux services de communications électroniques non publics.

⁷ Dans des contributions distinctes apportées après la clôture de la consultation publique, Europol et Eurojust ont toutefois plaidé en faveur d'une prise en compte des spécificités de leur travail en matière de coordination des services répressifs et de prévention de la criminalité.

contraignante, et une nouvelle base juridique a été créée⁸, qui permet l'élaboration d'une réglementation de l'Union complète et cohérente en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant, et de libre circulation de ces données. Cette nouvelle base juridique permet notamment à l'Union de réglementer la protection des données au moyen d'un seul instrument juridique, notamment dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale. La politique étrangère et de sécurité commune n'est que partiellement couverte par l'article 16 du TFUE, étant donné qu'une décision du Conseil, fondée sur une autre base juridique, doit établir des règles spécifiques applicables aux traitements de données effectués par les États membres dans ce domaine⁹.

S'appuyant sur ces nouvelles possibilités juridiques, la Commission accordera la priorité absolue au respect du droit fondamental à la protection des données dans l'ensemble de l'Union et dans toutes les politiques européennes, tout en renforçant la dimension «marché intérieur» de cette protection et en facilitant la libre circulation des données à caractère personnel. Dans ce contexte, il y a lieu de tenir pleinement compte d'autres droits fondamentaux pertinents consacrés dans la charte et d'autres objectifs énoncés dans les traités lorsqu'il s'agit de faire respecter le droit à la protection des données à caractère personnel.

La présente communication vise à définir l'approche qui permettra à la Commission de moderniser le cadre juridique de l'Union régissant la protection des données à caractère personnel dans tous ses domaines d'action, eu égard notamment aux défis posés par la mondialisation et les nouvelles technologies, de façon à continuer à garantir un niveau élevé de protection des personnes à l'égard du traitement de ces données dans tous ces domaines. L'Union pourra ainsi conserver un rôle moteur dans la promotion de normes strictes de protection des données dans le monde entier.

2. OBJECTIFS ESSENTIELS DE L'APPROCHE GLOBALE DE LA PROTECTION DES DONNEES

2.1. Renforcer les droits des personnes

2.1.1. Garantir aux personnes une protection adéquate en toutes circonstances

L'objectif des règles fixées dans les instruments européens actuels de protection des données est **de protéger les droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel les concernant**, conformément à la Charte des droits fondamentaux de l'Union européenne¹⁰.

La notion de «données à caractère personnel» est l'un des concepts clés de la protection des personnes par les instruments européens en vigueur dans le domaine de la protection des

⁸ Voir l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE).

⁹ Voir l'article 16, paragraphe 2, dernier alinéa, du TFUE et l'article 39 du traité sur l'Union européenne (TUE).

¹⁰ Voir l'arrêt de la Cour de justice dans l'affaire C-101/01, Bodil Lindqvist, Rec. 2003, p. I-1297, points 96 et 97, et dans l'affaire C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU, Rec. 2008, p. I-271. Voir également la jurisprudence de la Cour européenne des droits de l'homme, par exemple dans les affaires suivantes: S. et Marper contre Royaume-Uni, arrêt du 4.12.2008 (requête n^{os} 30562/04 et 30566/04); Rotaru contre Roumanie, arrêt du 4.5.2000 (requête n^{os} 28341/95), § 55, CEDH 2000-V.

données, et elle est à l'origine de l'imposition des obligations qui incombent aux responsables du traitement et aux sous-traitants¹¹. La définition du terme «données à caractère personnel» englobe l'ensemble des informations relatives à une personne identifiée ou identifiable, soit directement soit indirectement. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne¹². Cette approche délibérément choisie par le législateur présente l'avantage d'être souple, ce qui permet de l'appliquer à divers cas et évolutions touchant aux droits fondamentaux, y compris ceux qui n'étaient pas prévisibles au moment de l'adoption de la directive. Si elle est large et souple, elle comporte toutefois un inconvénient; en effet, dans de nombreux cas, lorsqu'il s'agit d'appliquer la directive, il n'est pas aisé de savoir quel point de vue adopter: soit celui des personnes concernées qui jouissent de droits en matière de protection des données, soit celui des responsables du traitement qui doivent satisfaire aux obligations imposées par la directive¹³.

Certaines situations impliquant le traitement d'informations spécifiques nécessiteraient l'adoption de mesures supplémentaires dans le cadre du droit de l'Union. De telles mesures existent déjà dans certains cas. Par exemple, le stockage de données dans un équipement terminal (par exemple, un téléphone portable) n'est autorisé que si la personne concernée y a consenti. Il pourrait être également nécessaire d'examiner cette question au niveau de l'Union en ce qui concerne, par exemple, les données codées, les données de localisation, les technologies d'exploration de données qui permettent de corréler des données émanant de sources différentes, ou dans les cas où il faut garantir la confidentialité et l'intégrité des systèmes d'information¹⁴.

Toutes les questions mentionnées ci-dessus nécessitent donc un examen minutieux.

La Commission envisagera **les manières de garantir une application cohérente des règles de protection des données, eu égard aux répercussions des nouvelles technologies sur les droits et libertés des personnes, et compte tenu de l'objectif consistant à assurer la libre circulation des données à caractère personnel dans le marché intérieur.**

2.1.2. *Accroître la transparence pour les personnes concernées*

La transparence est une condition fondamentale indispensable pour permettre aux personnes d'exercer un contrôle sur leurs propres données et pour assurer la protection effective des données à caractère personnel. Il est donc primordial que les responsables du traitement **informent** les personnes concernées **correctement et clairement, en toute transparence**, afin qu'elles sachent qui recueillera et traitera leurs données, selon quelles modalités, pour quels motifs et pendant combien de temps, et qu'elles connaissent leurs droits en ce qui concerne l'accès à ces données, leur rectification ou leur suppression. Les dispositions

¹¹ Voir les définitions des termes «responsable du traitement» et «sous-traitement» à l'article 2, points d) et e), de la directive 95/46/CE.

¹² Voir le considérant 26 de la directive 95/46/CE.

¹³ Voir, par exemple, le cas des adresses IP examiné dans l'avis 4/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel (document WP 136).

¹⁴ Voir, par exemple, la décision de la Cour constitutionnelle fédérale allemande (*Bundesverfassungsgericht*) du 27 février 2008, 1 BvR 370/07.

applicables relatives aux informations à communiquer à la personne concernée¹⁵ sont insuffisantes.

La transparence repose sur des éléments fondamentaux, tels qu'**un accès aisé à l'information, qui doit être facile à comprendre, et l'utilisation d'un langage clair et simple**. Cela est d'autant plus vrai dans un environnement en ligne où, bien souvent, les déclarations de confidentialité manquent de clarté, sont difficilement accessibles, peu transparentes¹⁶, et ne sont pas toujours pleinement conformes aux règles en vigueur. Un exemple pourrait être la publicité comportementale en ligne dans laquelle la multiplicité des intervenants et la complexité technologique sont telles que les internautes peuvent difficilement déterminer si des données à caractère personnel sont collectées, par qui et à quelle fin.

Dans ce contexte, les **enfants** méritent de faire l'objet d'une protection particulière, car ils peuvent être moins conscients des risques, des conséquences, des garanties et des droits liés au traitement de données à caractère personnel¹⁷.

La Commission envisagera les actions suivantes:

- introduire, dans le cadre juridique, un **principe général de transparence pour le traitement** des données à caractère personnel;
- soumettre les responsables du traitement à des **obligations spécifiques** quant au type d'informations à communiquer et aux **modalités** de leur communication, y compris en ce qui concerne les **enfants**;
- élaborer un ou plusieurs **modèles européens** («**déclarations de confidentialité**») à l'intention des responsables du traitement.

Il importe également que les intéressés soient informés lorsque des données les concernant ont été accidentellement ou illégalement détruites, perdues, altérées, consultées par des personnes non autorisées ou divulguées à de telles personnes. La récente révision de la directive «vie privée et communications électroniques» a instauré une **notification obligatoire des violations de données**, qui n'est toutefois applicable que dans le secteur des télécommunications. Vu le risque que des violations de données se produisent dans d'autres secteurs (par exemple, le secteur financier), la Commission examinera les modalités d'une extension à d'autres secteurs de l'obligation de notifier les atteintes aux données à caractère personnel, conformément à la déclaration qu'elle a présentée à cet égard au Parlement européen en 2009, dans le contexte de la réforme du cadre réglementaire relatif aux communications électroniques¹⁸. Cet examen n'aura aucune incidence sur les dispositions de

¹⁵ Voir les articles 10 et 11 de la directive 95/46/CE.

¹⁶ Un sondage Eurobaromètre réalisé en 2009 a révélé que la moitié des personnes interrogées estimaient que les déclarations de confidentialité figurant sur les sites web étaient peu claires, voire très peu claires (voir l'Eurobaromètre flash n° 282, en anglais uniquement: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

¹⁷ Voir l'étude qualitative intitulée «Internet plus sûr pour les enfants», concernant les enfants de 9 et 10 ans et de 12 à 14 ans, qui a révélé que les enfants ont tendance à sous-estimer les risques liés à l'utilisation de l'internet et à minimiser les conséquences de leurs éventuels comportements à risque (le rapport de synthèse en français est disponible à l'adresse suivante: http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2007/summary_report_fr.pdf).

¹⁸ «La Commission prend acte du souhait du Parlement européen que cette obligation de signaler les violations de données personnelles ne devrait pas se limiter au secteur des communications électroniques, mais qu'elle s'applique également à d'autres entités comme les prestataires de services de

la directive «vie privée et communications électroniques», qui doit être transposée en droit national au plus tard le 25 mai 2011¹⁹. Il y a lieu de garantir l'adoption d'une approche systématique et cohérente à cet égard.

La Commission engagera l'action suivante:

- examiner les modalités d'introduction, dans le cadre juridique global, d'une **obligation générale de notification des violations de données à caractère personnel**, indiquant les destinataires de ce type de notifications et les critères auxquels serait subordonnée l'application de cette obligation.

2.1.3. Permettre aux intéressés d'exercer un meilleur contrôle sur les données les concernant

Pour s'assurer que les personnes concernées bénéficient d'un niveau élevé de protection des données, deux conditions doivent au préalable être satisfaites: **le traitement des données par les responsables doit être limité à des finalités bien précises (principe de la minimisation des données)** et les intéressés doivent conserver la possibilité d'un **contrôle effectif sur les données les concernant**. Aux termes de l'article 8, paragraphe 2, de la charte, «[t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification». Chacun devrait toujours pouvoir accéder à ses données, les rectifier, les effacer ou les verrouiller, hormis si des motifs légitimes prévus par la loi s'y opposent. Ces droits sont déjà consacrés dans le cadre juridique actuel. Les modalités de leur exercice ne sont toutefois pas harmonisées, celui-ci étant donc effectivement plus aisé dans certains États membres que dans d'autres. Cette question se pose avec d'autant plus d'acuité en ce qui concerne l'environnement en ligne que des données y sont souvent conservées sans que la personne concernée n'en ait préalablement été informée et/ou sans qu'elle n'y ait consenti.

L'exemple des sites de socialisation est particulièrement éclairant à cet égard, car pour y exercer un contrôle effectif sur les données les concernant, les intéressés se heurtent à des défis de taille. La Commission a ainsi reçu plusieurs plaintes de personnes qui n'avaient pu récupérer des données à caractère personnel auprès de prestataires de services en ligne, telles que leurs photos, et qui ont donc été empêchées d'exercer leur droit d'accès, de rectification et de suppression.

Par conséquent, il convient d'explicitier, de clarifier, voire de renforcer ces droits.

la société de l'information [...]. La Commission lancera donc sans retard les travaux préparatoires appropriés, y compris une consultation des parties prenantes, afin de soumettre des propositions adéquates en la matière d'ici à la fin 2011 [...]; document consultable à l'adresse suivante: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//FR>. Voir également le considérant 59 de la directive 2009/136/CE modifiant la directive 2002/58/CE («vie privée et communications électroniques»): «L'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs.»

¹⁹

Voir l'article 4 de la directive 2009/136/CE.

La Commission étudiera donc les moyens permettant:

- de renforcer le **principe de la minimisation des données**;
- d'**améliorer les modalités** d'un véritable **exercice des droits d'accès, de rectification, de suppression et de verrouillage** (par exemple, en fixant des délais de réponse aux demandes des personnes concernées, en autorisant l'exercice de ces droits par voie électronique ou en instaurant la gratuité de principe de l'exercice du droit d'accès);
- de clarifier le «**droit à l'oubli**», c'est-à-dire le droit en vertu duquel les personnes peuvent obtenir l'arrêt du traitement des données les concernant et l'effacement de celles-ci lorsqu'elles ne sont plus nécessaires à des fins légitimes. Il s'agit, par exemple, du cas dans lequel la personne revient sur son consentement au traitement des données, ou du cas dans lequel le délai de conservation des données a expiré;
- de compléter l'éventail des droits des personnes concernées, en assurant la «**portabilité des données**», c'est-à-dire en conférant à l'intéressé le droit explicite de retirer ses données (par exemple, des photos ou une liste d'amis) d'une application ou d'un service, de sorte que les données ainsi retirées puissent être transférées vers une autre application ou un autre service, pour autant que cela soit techniquement réalisable, sans que les responsables du traitement n'y fassent obstacle.

2.1.4. *Sensibiliser*

Si la transparence est essentielle, il est également indispensable de sensibiliser davantage le grand public, et notamment les jeunes, aux risques liés au traitement de données à caractère personnel ainsi qu'aux droits dont ils jouissent. Un sondage Eurobaromètre réalisé en 2008 a révélé qu'une grande majorité des habitants des États membres de l'UE jugeaient plutôt faible le niveau de sensibilisation de leurs concitoyens à la protection des données à caractère personnel²⁰. Il conviendrait donc que les actions de sensibilisation soient encouragées et soutenues par toute une série d'acteurs, c'est-à-dire les autorités nationales, notamment celles qui sont chargées de la protection des données et les organismes de formation, ainsi que les responsables du traitement et les associations de la société civile. Ces actions devraient, entre autres, consister dans des mesures non législatives, telles que des campagnes de sensibilisation dans la presse écrite et les médias électroniques, la publication d'informations claires sur des sites web, qui décrivent précisément les droits des personnes concernées et les responsabilités des responsables du traitement.

La Commission étudiera:

- la possibilité de **cofinancer des actions de sensibilisation à la protection des données**, à l'aide du budget de l'Union;
- la nécessité et l'opportunité d'introduire dans le cadre juridique **une obligation de mener des actions de sensibilisation** dans ce domaine.

2.1.5. *Garantir un consentement éclairé et libre*

Lorsqu'un consentement éclairé est exigé, les règles en vigueur prévoient que l'accord de l'intéressé sur le traitement de données à caractère personnel le concernant devrait consister

²⁰ Voir l'Eurobaromètre flash n° 225 - La protection des données au sein de l'Union européenne: http://ec.europa.eu/public_opinion/flash/fl_225_fr.pdf

dans «toute manifestation de volonté, libre, spécifique et informée» par laquelle il accepte ce traitement²¹. Or actuellement, dans les États membres, ces conditions font l'objet d'interprétations diverses, allant de l'obligation générale d'obtenir un consentement écrit à l'acceptation d'un consentement implicite.

En outre, dans un environnement en ligne – vu l'opacité des politiques de protection de la vie privée – les personnes ont souvent plus de difficulté à s'informer sur leurs droits et à donner un consentement éclairé. Cela est d'autant plus complexe que, dans certains cas, l'on ne voit pas clairement ce qui constituerait un consentement libre, spécifique et éclairé à un traitement de données, comme dans le domaine de la publicité comportementale en ligne où certains considèrent, mais pas d'autres, que les paramètres du navigateur de l'internaute expriment son consentement.

Il conviendrait donc de clarifier les conditions du **consentement** de la personne concernée, afin de garantir qu'il est toujours **accordé en connaissance de cause**, et de s'assurer que l'intéressé est pleinement conscient qu'il donne son autorisation et sait de quel traitement il s'agit, conformément à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. La clarification des notions clés peut également favoriser les initiatives en matière d'autoréglementation visant à dégager des solutions pratiques conformes au droit de l'Union.

La Commission étudiera les moyens **de clarifier et de renforcer les règles en matière de consentement**.

2.1.6. *Protéger les données sensibles*

Le traitement des données sensibles, c'est-à-dire des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, sont déjà interdits en règle générale, des exceptions limitées étant autorisées sous réserve de certaines conditions et garanties²². Cependant, eu égard aux évolutions technologiques et sociétales, il faut revoir les dispositions existantes relatives aux données sensibles, afin de déterminer s'il conviendrait de soumettre d'autres catégories de données à cette réglementation et de préciser davantage les conditions applicables à leur traitement. Sont concernées, par exemple, les données génétiques qui, pour l'heure, ne sont pas expressément considérées comme une catégorie de données sensibles.

La Commission envisagera les actions suivantes:

- déterminer si d'autres catégories de données devraient être considérées comme «**sensibles**», par exemple, les données **génétiques**;
- préciser davantage et **harmoniser les conditions** à remplir pour procéder au traitement de certaines catégories de données sensibles.

2.1.7. *Renforcer l'efficacité des voies de recours et des sanctions*

Pour garantir le respect des règles de protection des données, il est primordial de disposer d'une **réglementation efficace en matière de voies de recours et de sanctions**. Nombreux

²¹ Cf. article 2, point h), de la directive 95/46/CE.

²² Cf. article 8 de la directive 95/46/CE.

sont les cas où la violation de ces règles, au détriment d'une personne, en touche également beaucoup d'autres se trouvant dans une situation semblable.

Par conséquent, la Commission engagera les actions suivantes:

- envisager la possibilité d'**accorder le pouvoir de saisir les juridictions nationales** aux autorités chargées de la protection des données et aux associations de la société civile, ainsi qu'à d'**autres groupements représentant les intérêts des personnes concernées**;
- évaluer la nécessité de **durcir les dispositions en vigueur en matière de sanctions**, par exemple en prévoyant expressément des sanctions pénales pour les violations graves des règles de protection des données, afin d'en renforcer l'efficacité.

2.2. Renforcer la dimension «marché intérieur»

2.2.1. *Accroître la sécurité juridique et garantir des conditions égales aux responsables du traitement*

La protection des données dans l'Union revêt **une dimension «marché intérieur»** notable, c'est-à-dire la nécessité d'assurer la libre circulation des données à caractère personnel entre les États membres au sein du marché intérieur. En conséquence, l'harmonisation des législations nationales apportée en la matière par la directive ne se limite pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète²³.

Parallèlement, la directive reconnaît aux États membres une marge de manœuvre dans certains domaines et elle les autorise à maintenir ou à introduire des régimes particuliers pour des situations spécifiques²⁴. Ces éléments, combinés au fait que les États membres appliquent parfois incorrectement la directive, sont à l'origine de **divergences entre les législations nationales la transposant, qui vont à l'encontre de l'un de ses objectifs principaux, à savoir la libre circulation des données à caractère personnel dans le marché intérieur**. Ce constat vaut pour de nombreux secteurs et contextes, par exemple lors du traitement de données à caractère personnel dans le contexte professionnel ou à des fins de santé publique. L'harmonisation insuffisante est effectivement l'un des principaux problèmes récurrents mis en évidence par les parties prenantes issues du secteur privé, et notamment par les acteurs économiques, car elle entraîne des coûts supplémentaires et alourdit la charge administrative. C'est surtout vrai pour les responsables du traitement qui sont établis dans plusieurs États membres et qui sont tenus de satisfaire aux obligations et pratiques de chacun d'eux. De plus, les divergences dans l'application de la directive par les États membres créent une insécurité juridique non seulement pour les responsables du traitement, mais aussi pour les personnes concernées, et risquent ainsi de compromettre la réalisation de l'objectif que la directive est supposée atteindre, à savoir un niveau équivalent de protection.

La Commission étudiera les moyens de **pousser plus loin l'harmonisation des règles de protection des données au niveau de l'UE**.

²³ Arrêt de la Cour de justice dans l'affaire C-101/01, Bodil Lindqvist, Rec. 2003, p. I-1297, points 96 et 97.

²⁴ Ibidem, point 97. Voir également le considérant 9 de la directive 95/46/CE.

2.2.2. Réduire la charge administrative

Si les conditions applicables s'uniformisent, les responsables du traitement n'auront plus à se conformer à des exigences nationales divergentes, ce qui allégera considérablement la charge administrative qu'ils supportent. Une autre façon de réduire concrètement leur charge administrative et leurs coûts consisterait à **revoir et à simplifier le système actuel de notification**²⁵. La plupart des responsables du traitement s'accordent à dire que l'obligation générale actuelle de notifier toutes les opérations de traitement aux autorités chargées de la protection des données est assez lourde et n'apporte pas, en soi, de réelle valeur ajoutée sous l'angle de la protection des données à caractère personnel. Par ailleurs, il s'agit d'un domaine dans lequel la directive laisse une certaine marge de manœuvre aux États membres, qui sont libres de décider d'éventuelles exemptions et simplifications, ainsi que d'arrêter les procédures à suivre.

L'harmonisation et la simplification du système permettraient de réduire les coûts et la charge administrative, en particulier pour les entreprises multinationales établies dans plusieurs États membres.

La Commission étudiera les différents moyens de simplifier et d'harmoniser le système actuel de notification, y compris l'établissement éventuel d'un formulaire d'enregistrement uniforme valable dans toute l'Union.

2.2.3. Clarifier les règles relatives au droit applicable et à l'État membre responsable

Le premier rapport de la Commission sur la mise en œuvre de la directive relative à la protection des données soulignait, dès 2003²⁶, que la mise en œuvre de la disposition relative au droit applicable²⁷ posait «problème dans plusieurs cas, avec pour résultat l'apparition possible du type de conflit de lois que cet article cherche justement à éviter». La situation ne s'est pas améliorée depuis lors, si bien que les responsables du traitement et les autorités de contrôle de la protection des données ne savent pas toujours clairement quel est l'État membre responsable et quel est le droit applicable lorsque plusieurs États membres sont concernés. Tel est notamment le cas lorsque le responsable du traitement est soumis à des exigences différentes de la part des divers États membres, lorsqu'une entreprise multinationale est établie dans plusieurs États membres ou lorsque le responsable du traitement n'est pas établi dans l'Union, mais fournit ses services à des résidents de l'UE.

Une complexité croissante en raison de la mondialisation et des progrès technologiques: les responsables du traitement sont de plus en plus amenés à exercer leur activité dans plusieurs pays et juridictions et à fournir des services et prêter assistance 24 heures sur 24. L'internet permet aux responsables du traitement établis en dehors de l'Espace économique européen (EEE)²⁸ de fournir plus facilement des services à distance et de traiter en ligne des données à caractère personnel. Il est ainsi souvent difficile de localiser ces données et l'équipement utilisé (par exemple, dans les applications et services relevant de l'«informatique en nuage»).

²⁵ Voir l'article 18 de la directive 95/46/CE.

²⁶ Rapport de la Commission - Premier Rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) [COM(2003) 265].

²⁷ Voir l'article 4 de la directive 95/46/CE.

²⁸ L'Espace économique européen comprend la Norvège, le Liechtenstein et l'Islande.

Cependant, la Commission considère que même si le traitement des données à caractère personnel est confié à un responsable établi dans un pays tiers, les intéressés doivent pouvoir bénéficier de la protection à laquelle ils ont droit en vertu de la Charte des droits fondamentaux de l'Union européenne et de la législation de l'UE en matière de protection des données.

La Commission examinera la manière dont les **dispositions existantes sur le droit applicable pourraient être révisées et clarifiées**, notamment les critères actuels de détermination du droit applicable, en vue d'améliorer la sécurité juridique, de clarifier quel est l'État membre responsable de l'application des règles en matière de protection des données et, en définitive, d'assurer le même niveau de protection à tous les résidents de l'Union concernés, indépendamment du lieu d'établissement du responsable du traitement.

2.2.4. Responsabiliser davantage les responsables du traitement

La simplification administrative **ne devrait pas se traduire par une réduction générale du niveau de responsabilité des responsables du traitement à l'égard de la protection des données**. La Commission estime, au contraire, que leurs obligations devraient être définies plus clairement dans le cadre juridique, notamment en ce qui concerne les mécanismes de contrôle interne et la coopération avec les autorités de contrôle de la protection des données. En outre, il conviendrait de veiller à ce que ce niveau de responsabilité s'applique également aux responsables du traitement qui sont soumis au secret professionnel (par exemple, les avocats) et aux cas de plus en plus courants dans lesquels le responsable confie le traitement à une autre entité (par exemple, un sous-traitant).

La Commission étudiera donc les moyens de **garantir que les responsables du traitement mettent en place des politiques et mécanismes efficaces pour assurer le respect des règles en matière de protection des données**. Ce faisant, elle tiendra compte du débat actuel sur l'introduction possible d'un principe de l'«accountability»²⁹. Il ne s'agirait pas d'alourdir la charge administrative pesant sur les responsables du traitement, puisque ces mesures viseraient plutôt à mettre en place des garanties et des mécanismes de protection plus efficaces, tout en réduisant et en simplifiant certaines formalités administratives, telles que les notifications (voir la section 2.2.2 ci-dessus).

La promotion de l'utilisation des technologies d'amélioration de la confidentialité (PET), ainsi que le soulignait déjà la communication de la Commission de 2007 à ce sujet, ainsi que du principe de prise en compte du respect de la vie privée dès la conception («*Privacy by Design*») pourrait jouer un rôle important à cet égard, y compris pour garantir la sécurité des données³⁰.

La Commission examinera les mesures suivantes destinées à responsabiliser davantage les responsables du traitement:

²⁹ Voir, notamment, l'avis n° 3/2010 du groupe de travail «Article 29» adopté le 13 juillet 2010.

³⁰ S'agissant des PET, voir: communication de la Commission au Parlement européen et au Conseil sur la promotion de la protection des données à l'aide de technologies d'amélioration de la confidentialité ou PET (*Privacy Enhancing Technologies*) [COM(2007) 228 final]. Le principe de «*Privacy by Design*» signifie que la protection de la vie privée et des données à caractère personnel est prise en compte tout au long du cycle de vie des technologies, depuis le stade de leur conception jusqu'à leur déploiement, utilisation et élimination finale. Ce principe figure notamment dans la communication de la Commission intitulée «Une stratégie numérique pour l'Europe» [COM(2010) 245].

- rendre obligatoire la désignation d'un **responsable du traitement** indépendant, et harmoniser les règles relatives à leurs tâches et compétences³¹, tout en évitant de faire peser des charges administratives indues, notamment sur les petites et microentreprises;
- introduire dans le cadre juridique l'obligation, pour les responsables du traitement, de réaliser une **analyse d'impact au regard de la protection des données** dans certains cas, par exemple lorsque des données sensibles sont traitées ou lorsque le type de traitement comporte des risques spécifiques, notamment dans le cas de l'utilisation de technologies, mécanismes ou procédures spécifiques, tels que le profilage ou la vidéosurveillance;
- poursuivre la promotion de l'utilisation des PET et des possibilités d'application concrète de la notion de «**prise en compte du respect de la vie privée dès la conception**».

2.2.5. *Encourager les initiatives en matière d'autoréglementation et examiner la possibilité d'instaurer des régimes européens de certification*

La Commission persiste à penser que les **initiatives en matière d'autoréglementation** prises par les responsables du traitement peuvent **contribuer à une meilleure application des règles relatives à la protection des données**. Les dispositions actuelles de la directive sur la protection des données concernant l'autoréglementation, à savoir la possibilité d'élaborer des codes de conduite³², ont rarement été appliquées jusqu'à présent et ne sont pas jugées satisfaisantes par les parties prenantes du secteur privé.

En outre, la Commission examinera la possibilité d'instaurer des **régimes européens de certification (par exemple, des «labels de protection de la vie privée»)** pour les processus, technologies, produits et services conformes aux normes de protection de la vie privée³³. Ceux-ci non seulement guideraient les personnes utilisant ces technologies, produits et services, mais responsabiliseraient aussi les responsables du traitement: la certification des technologies, produits ou services pourrait permettre de prouver que le responsable du traitement a effectivement rempli ses obligations (*voir la section 2.2.4 ci-dessus*). Il y aurait lieu, de toute évidence, de **garantir la fiabilité de tels labels de protection de la vie privée** ainsi que leur compatibilité avec les obligations légales et les normes techniques internationales.

La Commission entend:

- examiner les moyens **d'encourager davantage les initiatives en matière d'autoréglementation**, notamment la promotion active des codes de conduite;
- étudier la faisabilité de l'instauration de **régimes européens de certification** dans le domaine de la protection de la vie privée et des données.

³¹ La possibilité actuelle, donnée au responsable du traitement, de désigner un correspondant à la protection des données pour veiller, en toute indépendance, au respect des règles nationales et de l'UE en matière de protection des données et pour aider les personnes concernées a déjà été utilisée dans plusieurs États membres (voir, par exemple, le «*Beaufragter für den Datenschutz*» en Allemagne et le «correspondant informatique et libertés (CIL)» en France).

³² Voir l'article 27 de la directive 95/46/CE.

³³ Voir également, à cet égard, la communication sur les PET citée à la note de bas de page n° 30.

2.3. Réviser les règles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale

La directive sur la protection des données s'applique à toutes les activités de traitement de données à caractère personnel, tant dans le secteur public que dans le secteur privé. Cependant, elle ne s'applique pas au «traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire», telles que les activités dans les domaines de la coopération policière et judiciaire en matière pénale³⁴. Le traité de Lisbonne a toutefois supprimé l'ancienne «structure en piliers» de l'UE et introduit une nouvelle base juridique complète pour la protection des données à caractère personnel dans toutes les politiques de l'Union³⁵. Dans ce contexte et compte tenu de la Charte des droits fondamentaux de l'Union européenne, les communications de la Commission concernant respectivement le programme de Stockholm et le plan d'action mettant en œuvre le programme de Stockholm³⁶ ont souligné la nécessité de mettre en place «un régime complet de protection» et de «durcir la position de l'UE en matière de protection des données à caractère personnel dans le cadre de toutes les politiques européennes, y compris dans les domaines répressif et de la prévention de la criminalité».

L'instrument de l'UE applicable en matière de protection des données à caractère personnel dans les domaines de la coopération policière et judiciaire en matière pénale est la **décision-cadre 2008/977/JAI**³⁷. Cette dernière a constitué une avancée importante dans un domaine où le besoin de normes communes pour la protection des données devenait criant. Il convient toutefois d'aller encore plus loin.

La décision-cadre ne s'applique qu'à l'échange transfrontière de données à caractère personnel dans l'UE et, partant, pas aux opérations de traitement nationales effectuées dans les États membres³⁸. Cette distinction est difficile à établir dans la pratique et peut compliquer la mise en œuvre et l'application effectives de la décision-cadre.

La décision-cadre prévoit une dérogation trop large au principe de limitation de la finalité. Une autre de ses lacunes est l'absence de dispositions prévoyant une différenciation des diverses catégories de données en fonction de leur degré d'exactitude ou de fiabilité, et en particulier une différenciation des données fondées sur des faits de celles fondées sur des opinions ou appréciations personnelles³⁹, ainsi qu'une différenciation des diverses catégories de personnes concernées (délinquants, suspects, victimes, témoins, etc.), assortie de garanties spécifiques pour les données relatives à des personnes non soupçonnées⁴⁰.

³⁴ Voir l'article 3, paragraphe 2, premier tiret, de la directive 95/46/CE.

³⁵ Voir l'article 16 du TFUE.

³⁶ Voir les COM(2009) 262 du 10.6.2009 et COM(2010) 171 du 20.4.2010.

³⁷ 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). Cette décision-cadre n'envisage qu'une harmonisation minimale des normes de protection des données.

³⁸ Cette distinction n'existe pas dans les instruments pertinents du Conseil de l'Europe tels que la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), et la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée par le Conseil de l'Europe le 17 septembre 1987.

³⁹ Ainsi que l'exige le principe 3.2 de la recommandation n° R (87) 15.

⁴⁰ Contraire au principe 2 de la recommandation n° R (87) 15 et à ses rapports d'évaluation.

Qui plus est, **la décision-cadre ne remplace pas les divers instruments législatifs de nature sectorielle qui ont été adoptés au niveau de l'Union dans les domaines de la coopération policière et judiciaire en matière pénale**⁴¹, notamment ceux qui régissent le fonctionnement d'Europol, d'Eurojust, du système d'information Schengen (SIS) et du système d'information des douanes (SID)⁴², qui prévoient des régimes particuliers de protection des données et/ou généralement renvoient à des instruments de protection des données du Conseil de l'Europe. En ce qui concerne les activités dans le cadre de la coopération policière et judiciaire, tous les États membres ont souscrit à la recommandation du Conseil de l'Europe n° R (87) 15, qui définit les principes de la convention n° 108 pour le secteur de la police. Cette recommandation ne constitue toutefois pas un instrument juridiquement contraignant.

Cette situation peut porter directement atteinte aux possibilités des personnes d'exercer leurs droits en matière de protection des données dans ces domaines (par exemple, le droit de savoir quelles données à caractère personnel les concernant sont traitées et échangées, par qui et à quelles fins, et celui de connaître les modalités d'exercice de ces droits, tels que le droit d'accès aux données les concernant).

L'objectif consistant à mettre en place un système global et cohérent dans l'UE et à l'égard des pays tiers exige donc d'envisager **une révision des règles actuelles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale**. La Commission souligne que la notion de régime global de protection des données n'exclut pas l'adoption de règles spécifiques pour les secteurs judiciaire et de la police à l'intérieur du cadre général, compte tenu de la nature spécifique de ces domaines, ainsi que l'indique la déclaration 21 annexée au traité de Lisbonne. Cela implique, par exemple, d'examiner dans quelle mesure l'exercice par une personne de certains droits en matière de protection des données peut, dans un cas donné, compromettre la prévention, la détection ou la poursuite d'infractions pénales, les enquêtes correspondantes, ou encore l'exécution de sanctions pénales.

La Commission s'attachera notamment à:

- examiner l'opportunité **d'étendre l'application des règles générales de protection des données aux domaines de la coopération policière et de la coopération judiciaire en matière pénale, y compris pour le traitement au niveau national**, tout en prévoyant au besoin des **limitations harmonisées à certains droits** des personnes, par exemple en ce qui concerne le droit d'accès ou le principe de transparence;
- examiner la nécessité d'introduire des **dispositions spécifiques et harmonisées** dans le nouveau cadre général régissant la protection des données, par exemple en ce qui concerne le traitement des **données génétiques** à des fins répressives ou la distinction à établir entre les diverses catégories de personnes concernées (témoins, suspects, etc.) dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale;

⁴¹ Voir la présentation générale de ces instruments dans la communication de la Commission intitulée «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice» [COM(2010) 385].

⁴² Des autorités de contrôle communes ont été instituées par les instruments correspondants afin d'assurer le contrôle de la protection des données, en plus des pouvoirs de contrôle généraux conférés par le règlement (CE) n° 45/2001 au contrôleur européen de la protection des données (CEPD) sur les institutions, organes, bureaux et agences de l'Union.

- engager, en 2011, une **consultation** de toutes les parties intéressées sur la meilleure manière de **réviser les systèmes de contrôle actuels dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale**, afin de garantir l'exercice d'un contrôle efficace et cohérent de la protection des données sur l'ensemble des institutions, organes, bureaux et agences de l'Union;

- évaluer la nécessité d'**aligner**, à long terme, les **diverses règles sectorielles, adoptées au niveau de l'UE pour la coopération policière et judiciaire en matière pénale et contenues dans des instruments spécifiques**, avec le nouveau cadre juridique général de la protection des données.

2.4. La dimension mondiale de la protection des données

2.4.1. Clarifier et simplifier les règles applicables aux transferts internationaux de données

Le transfert de données à caractère personnel en dehors de l'UE et de l'espace EEE est notamment subordonné à l'«**évaluation du caractère adéquat**» du niveau de protection assuré par le pays tiers concerné, lequel peut actuellement être apprécié par la Commission et par les États membres.

Lorsque la Commission juge adéquat le niveau de protection assuré par un pays tiers, les données à caractère personnel peuvent alors circuler librement des vingt-sept États membres de l'UE et des trois pays membres de l'EEE vers ce pays tiers, sans qu'aucune autre garantie ne soit nécessaire. Cependant, les conditions exactes à remplir pour que la Commission reconnaisse le caractère adéquat du niveau de protection ne sont pas actuellement définies d'une manière suffisamment précise dans la directive sur la protection des données. En outre, la décision-cadre ne prévoit pas l'adoption de ce type de décision par la Commission.

Dans certains États membres, le caractère adéquat du niveau de protection est évalué en premier lieu par le responsable du traitement qui transfère lui-même des données à caractère personnel à un pays tiers, parfois dans le cadre du contrôle ex post effectué par l'autorité de contrôle de la protection des données. Cette situation peut donner lieu à des approches différentes de l'appréciation du niveau de protection assuré par les pays tiers, ou bien les organisations internationales, et, partant, **comporte le risque que le niveau de protection des personnes concernées prévu dans un pays tiers soit jugé différemment d'un État membre à l'autre**. Or les instruments juridiques existants ne définissent pas de conditions précises et harmonisées quant aux transferts pouvant être considérés comme licites. Aussi les pratiques varient-elles d'un État membre à l'autre.

De plus, en ce qui concerne les transferts vers des pays tiers qui n'assurent pas un niveau de protection adéquat, les clauses types actuelles de la Commission pour le transfert de données à caractère personnel aux responsables du traitement⁴³ et aux sous-traitants⁴⁴ ne sont pas

⁴³ Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (JO L 181 du 4.7.2001, p. 19); décision 2002/16/CE de la Commission du 27 décembre 2001 du 27 décembre 2001 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 (JO L 6 du 10.1.2002, p. 52); décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers (JO L 385 du 29.12.2004, p. 74).

conçues pour des situations non contractuelles et ne peuvent pas, par exemple, être appliquées à des transferts entre administrations publiques.

Qui plus est, les accords internationaux conclus par l'UE ou ses États membres exigent souvent l'insertion de clauses spécifiques ou de principes relatifs à la protection des données. Cela peut aboutir à des textes divers prévoyant des dispositions et des droits incohérents et, partant, se prêtant à des interprétations divergentes, aux dépens de la personne concernée. En conséquence, la Commission a annoncé qu'elle travaillerait sur les éléments essentiels relatifs à la protection des données à caractère personnel que doivent comporter les accords conclus à des fins répressives entre l'Union et des pays tiers⁴⁵.

D'autres moyens prenant la forme d'une autoréglementation, tels que les codes de conduite internes de certaines entreprises («*règles d'entreprise contraignantes*»)⁴⁶, peuvent également constituer un outil utile pour les transferts licites de données à caractère personnel entre les entreprises d'un même groupe. Toutefois, les parties prenantes ont laissé entendre que ce mécanisme pouvait être encore amélioré et sa mise en œuvre facilitée.

Eu égard aux problèmes mis en évidence, **il y a lieu d'améliorer, d'une manière générale, les mécanismes existants de transfert international de données à caractère personnel**, tout en garantissant un niveau adéquat de protection de ces données en cas de transfert ou de traitement en dehors de l'UE ou de l'EEE.

La Commission entend examiner les moyens:

- d'**améliorer et de rationaliser les procédures actuelles** de transfert international de données, y compris les instruments juridiquement contraignants et les «*règles d'entreprise contraignantes*», afin de parvenir à une **approche de l'UE plus uniforme et plus cohérente** à l'égard des pays tiers et des organisations internationales;
- de **clarifier sa procédure d'évaluation du caractère adéquat du niveau de protection assuré dans un pays tiers ou une organisation internationale et de préciser les critères et conditions** applicables;
- de définir les **éléments essentiels en matière de protection des données** que devraient comporter tous les types d'accords internationaux conclus par l'UE.

2.4.2. Promouvoir des principes universels

Étant mondialisé, le traitement des données appelle l'élaboration de règles universelles en matière de protection des personnes à l'égard du traitement des données à caractère personnel.

⁴⁴ Décision de la Commission 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 (JO L 39 du 12.2.2010, p. 5).

⁴⁵ Plan d'action mettant en œuvre le programme de Stockholm, voir la note de bas de page n° 36 ci-dessus.

⁴⁶ On entend par «*règles d'entreprise contraignantes*» des codes de bonne pratique fondés sur les normes européennes de protection des données, que les multinationales établissent et suivent volontairement pour garantir un niveau adéquat de protection des données transférées. Au sujet des catégories de transferts de données à caractère personnel entre les entreprises d'un même groupe et liées par les mêmes règles internes, voir:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Le cadre juridique de l'UE en la matière a souvent servi de **référence aux pays tiers pour réglementer la protection des données**. Son incidence et ses effets, tant à l'intérieur qu'en dehors de l'Union, ont été de la plus haute importance. **L'Union européenne doit donc continuer de jouer un rôle moteur dans l'élaboration et la promotion des normes juridiques et techniques internationales dans le domaine de la protection des données à caractère personnel, sur la base des instruments pertinents de l'UE et des autres instruments européens** relatifs à la protection des données. Cela est tout particulièrement important dans le cadre de la politique d'élargissement de l'UE.

En ce qui concerne les normes techniques internationales élaborées par les organismes de normalisation, la Commission considère qu'une cohérence entre le futur cadre juridique et ces normes sera essentielle pour assurer une mise en œuvre systématique et pratique des règles de protection des données par les responsables du traitement.

La Commission entend:

- continuer de **promouvoir l'élaboration de normes juridiques et techniques élevées en matière de protection des données dans les pays tiers et au niveau international**;
- s'efforcer de défendre le **principe de réciprocité de la protection dans les actions internationales de l'Union et notamment en ce qui concerne les personnes dont les données sont exportées de l'UE vers des pays tiers**;
- **renforcer sa coopération, à cette fin, avec les pays tiers et les organisations internationales**, tels que l'OCDE, le Conseil de l'Europe, les Nations unies, et d'autres organisations régionales;
- **suivre de près l'élaboration des normes techniques internationales par les organismes de normalisation** tels que le CEN et l'ISO, afin de s'assurer qu'elles complètent utilement les règles juridiques et respectent effectivement sur le plan opérationnel les exigences essentielles en matière de protection des données.

2.5. Renforcer le cadre institutionnel en vue d'un plus grand respect des règles de protection des données

L'application et le contrôle de l'application des principes et des règles en matière de protection des données sont indispensables pour garantir le respect des droits des personnes concernées.

Dans ce contexte, **le rôle des autorités chargées de la protection des données (DPA) est essentiel** pour le contrôle de l'application des règles de protection des données. Ces autorités sont les gardiennes indépendantes des libertés et des droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel les concernant. C'est pourquoi la Commission estime que leur rôle devrait être renforcé, eu égard notamment à la jurisprudence récente de la Cour de justice de l'Union européenne concernant leur indépendance⁴⁷, et qu'elles devraient être dotées des pouvoirs et des ressources nécessaires pour accomplir correctement leurs tâches tant au niveau national que lorsqu'elles coopèrent les unes avec les autres.

⁴⁷ Arrêt du 9 mars 2010 dans l'affaire C-518/07, Commission/Allemagne.

Parallèlement, la Commission considère que **les autorités de protection des données devraient renforcer leur coopération et mieux coordonner leurs activités**, notamment lorsqu'elles rencontrent des problèmes qui revêtent, par nature, une dimension transfrontière. Cela est tout particulièrement le cas lorsque des entreprises multinationales sont établies dans plusieurs États membres et exercent leurs activités dans chacun de ces États, ou lorsqu'un contrôle coordonné avec le contrôleur européen de la protection des données (CEPD) est requis⁴⁸.

À cet égard, **un rôle important peut être joué par le groupe de travail «article 29»⁴⁹**, qui a déjà pour tâche, en plus de sa fonction consultative⁵⁰, de contribuer à l'application uniforme des règles de protection des données de l'UE au niveau national. Cependant, l'application et l'interprétation sans cesse divergentes des règles de l'UE par les autorités de protection des données, même si les défis dans ce domaine sont les mêmes dans toute l'Union, appellent un renforcement du rôle de ce groupe de travail dans la coordination des positions des DPA, en vue de garantir une application plus uniforme au niveau national et, partant, un niveau équivalent de protection des données.

La Commission examinera les moyens:

- de **renforcer, clarifier et harmoniser le statut et les pouvoirs des autorités nationales de protection des données** dans le nouveau cadre juridique, y compris la pleine mise en œuvre de la notion d'«indépendance complète»⁵¹;
- d'**améliorer la coopération et la coordination entre les autorités de protection des données**;
- de **garantir une application plus cohérente des règles de l'UE en matière de protection des données dans tout le marché intérieur, notamment en renforçant le rôle des contrôleurs nationaux de la protection des données, en coordonnant mieux leur action par l'intermédiaire du groupe de travail «article 29» (qui devrait devenir un organe plus transparent), et/ou en créant un mécanisme destiné à assurer une cohérence dans le marché intérieur sous l'autorité de la Commission européenne.**

3. CONCLUSION: PERSPECTIVES

Comme les technologies, l'utilisation et le partage des données à caractère personnel dans nos sociétés sont en évolution constante. Le défi ainsi posé aux législateurs est celui de la mise en place d'un cadre législatif qui résistera à l'épreuve du temps. Au terme du processus de réforme, les règles européennes de protection des données devraient continuer de garantir un

⁴⁸ Tel est actuellement le cas pour les systèmes d'information à grande échelle, par exemple pour le SIS II (cf. article 46 du règlement (CE) n° 1987/2006 – JO L 318 du 28.12.2006, p. 4) et pour le VIS (cf. article 43 du règlement (CE) n° 767/2008 - JO L 218 du 13.8.2008, p. 60).

⁴⁹ Le groupe de travail «Article 29» est un organe consultatif composé d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant du contrôleur européen de la protection des données (CEPD) et d'un représentant de la Commission (sans droit de vote). Son secrétariat est assuré par les services de la Commission. Voir: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

⁵⁰ Le groupe de travail «Article 29» a pour mission de donner à la Commission un avis sur le niveau de protection dans l'UE et dans les pays tiers, ainsi que sur toute autre mesure relative au traitement des données à caractère personnel.

⁵¹ Voir l'arrêt du 9 mars 2010 dans l'affaire C-518/07, Commission/Allemagne.

niveau élevé de protection et d'assurer la sécurité juridique aux personnes, aux administrations publiques et aux entreprises dans le marché intérieur. Peu importe la complexité de la situation ou le caractère sophistiqué de la technologie, il est essentiel que les règles et les normes applicables, que les autorités nationales doivent faire appliquer et auxquelles les entreprises et les développeurs de technologies doivent se conformer, soient définies clairement. De même, les droits conférés aux personnes devraient être clairs pour les intéressés.

L'approche globale envisagée par la Commission pour remédier aux problèmes et atteindre les objectifs essentiels mis en évidence dans la présente communication servira de base aux discussions ultérieures avec les autres institutions européennes et les autres parties intéressées. Elle sera ensuite traduite en propositions et mesures concrètes de nature à la fois législative et non législative. À cette fin, la Commission souhaiterait recevoir un retour d'informations sur les questions soulevées dans la présente communication.

Sur cette base, à la suite d'une analyse d'impact et compte tenu de la Charte des droits fondamentaux de l'Union européenne, la Commission **présentera en 2011 des propositions législatives** destinées à réviser le cadre juridique de la protection des données, afin de durcir la position de l'UE en matière de protection des données à caractère personnel dans le cadre de toutes les politiques européennes, y compris dans les domaines répressif et de la prévention de la criminalité, eu égard aux spécificités de ces domaines. Les mesures non législatives, telles que la promotion de l'autoréglementation et l'examen de la faisabilité des «labels européens de protection de la vie privée», seront prises parallèlement.

Dans un deuxième temps, la Commission **évaluera la nécessité d'adapter d'autres instruments juridiques** au nouveau cadre général de la protection des données. Cela concerne tout d'abord le règlement (CE) n° 45/2001 dont les dispositions devront faire l'objet d'une adaptation. Il conviendra également, à un stade ultérieur, d'examiner avec attention l'impact sur les autres instruments sectoriels.

La Commission continuera également de contrôler la bonne application du droit de l'Union dans ce domaine, en poursuivant une **politique volontariste de répression des infractions** lorsque les règles de l'UE en matière de protection des données ne seront pas mises en œuvre et appliquées correctement. En effet, le réexamen actuel des instruments pertinents ne porte nullement atteinte à l'obligation des États membres de mettre en œuvre les instruments juridiques existant en matière de protection des données à caractère personnel et de veiller à leur bonne application⁵².

C'est en assurant un niveau élevé et uniforme de protection des données dans l'Union que nous serons le mieux à même de défendre et de promouvoir au niveau mondial les normes européennes en la matière.

⁵² Au nombre de ces instruments figure la décision-cadre 2008/977/JAI de la Commission, à laquelle les États membres doivent se conformer avant le 27 novembre 2010.