COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 7.3.2007
COM(2007) 87 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données

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

La directive 95/46/CE[1] a marqué une étape importante dans l'histoire de la protection des données à caractère personnel en tant que droit fondamental, dans le droit fil de la Convention 108 du Conseil de l'Europe[2]. Établi en application de l'article 33 de la directive, le premier rapport de la Commission sur sa mise en œuvre[3] concluait qu'il n'était pas opportun de prévoir des modifications législatives, mais que des actions devaient être entreprises et qu'il subsistait une marge de manœuvre considérable pour améliorer l'application de ladite directive.

Le rapport contenait un *Programme de travail pour une meilleure mise en application de la directive sur la protection des données*. La présente communication examine le travail réalisé dans le cadre de ce programme, évalue la situation actuelle et esquisse les perspectives futures en tant que condition préalable au succès dans une série de domaines d'action, à la lumière de l'article 8 de la Charte européenne des droits fondamentaux, qui reconnaît un droit autonome à la protection des données à caractère personnel.

La Commission estime que la directive établit un cadre juridique général adéquat dans l'ensemble et techniquement neutre. L'ensemble des règles harmonisées assurant un degré élevé de protection des données à caractère personnel dans l'UE a procuré des avantages considérables aux citoyens, aux entreprises et aux autorités. Ces règles protègent les particuliers contre la surveillance générale ou les discriminations injustifiées fondées sur les informations les concernant détenues par autrui. La confiance que les consommateurs fondent dans le fait que les données personnelles transmises au cours des transactions ne feront pas l'objet d'une utilisation frauduleuse, est une condition du développement du commerce électronique. Les entreprises exercent leurs activités et les administrations coopèrent dans toute la Communauté, sans craindre que leurs activités internationales soient interrompues en raison d'un manque de protection, au départ ou à l'arrivée, des données à caractère personnel qu'elles doivent échanger.

La Commission continuera de suivre la mise en œuvre de la directive, collaborera avec tous les acteurs pour réduire davantage les divergences nationales et examinera la nécessité d'une législation sectorielle pour appliquer les principes de protection des données aux nouvelles technologies et répondre aux exigences de la sécurité publique.

---

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), ci-après «la directive».

2 STE n° 108; ci-après «la Convention 108».

3 Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), COM(2003) 265 final, du 15.5.2003.

1. LE PASSÉ: RÉALISATIONS DANS LE CADRE DU PROGRAMME DE TRAVAIL

Depuis la publication du rapport, des actions ont été menées dans les dix domaines suivants[4].

Action 1: Discussions avec les États membres et les autorités chargées de la protection des données

La Commission mène avec les États membres un dialogue structuré en ce qui concerne la transposition au niveau national, qui englobe l'analyse détaillée de la législation nationale et des discussions avec les autorités nationales, afin de rendre celle-ci totalement conforme aux exigences de la directive.

Action 2: Association des pays candidats aux efforts visant à une mise en application de meilleure qualité et plus uniforme de la directive

Des représentants de ces États membres ont participé avant l'adhésion aux réunions du comité institué en vertu de l'article 31 de la directive, comme ils le faisaient avec le groupe de travail «Article 29»[5] depuis 2002. Entre-temps, la Commission a travaillé en étroite collaboration avec les autorités de ces États membres dans le cadre de la procédure d'adoption de la législation nationale, offrant ses conseils pour la mise en conformité avec l'acquis, afin de limiter autant que possible les procédures d'infraction.

Action 3: Amélioration de la notification de l'ensemble des actes légaux transposant la directive et notification des autorisations accordées en vertu de l'article 26, paragraphe 2, de la directive

Le dialogue structuré mené dans le cadre de l'action 1 a permis à la Commission d'avoir une vision plus claire et plus complète des mesures nationales de transposition de la directive, y compris la législation secondaire et sectorielle. Dans une lettre envoyée aux États membres en août 2003, la Commission a proposé des critères communs pour un traitement pragmatique des notifications au titre de l'article 26, paragraphe 3, de la directive. Il en est résulté une augmentation des notifications faites par certains États membres. L'échange de bonnes pratiques et de connaissances entre les autorités nationales s'est intensifié après la publication sur le site internet de la Commission d'une sélection de documents d'orientation et des principales décisions et recommandations adoptées au niveau national.

Action 4: Respect de la directive

Dans sa déclaration concernant la mise en application de la directive, le groupe de travail a consacré le principe d'actions nationales synchronisées à mener au niveau de l'UE pour l'application de la directive et il a défini des critères pour aider à recenser les domaines dans lesquels une enquête devrait être réalisée. En mars 2006, les autorités nationales responsables de la protection des données ont lancé une enquête commune concernant le traitement des données à caractère personnel dans le secteur de l'assurance maladie privée.

---

4 Le premier rapport de la Commission, ainsi que d'autres documents publics adoptés dans le cadre du programme de travail mentionné dans la présente communication peuvent être consultés sur le site: http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm.

5 Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive, ci-après «groupe de travail».

Action 5: Notification et publicité des opérations de traitement

Le groupe de travail a préparé un rapport sur cette question, dans lequel il passe en revue les situations nationales existantes et formule des recommandations s'inspirant de celles de la Commission. Le *Vademecum on Notification Requirement* qui a suivi, visait à faire le tour des différentes dispositions nationales et à recommander des bonnes pratiques et des orientations aux responsables du traitement.

Action 6: Dispositions davantage harmonisées en matière d'information

Outre l'analyse des législations nationales que la Commission a réalisée dans le cadre du dialogue structuré, le groupe de travail a reconnu la nécessité d'une harmonisation et a cherché à définir une approche commune pour l'élaboration d'une solution pragmatique. Il a fourni aux responsables du traitement des lignes directrices concernant certains cas concrets, sur le contenu et la forme des informations et sur les modèles d'avis sur la protection de la vie privée à différents niveaux ou les avis relatifs au transfert de données PNR.

Action 7: Simplification des obligations en matière de transferts internationaux

a) Utilisation plus large des constatations relatives à la protection adéquate dans les pays tiers au titre de l'article 25, paragraphe 6

Depuis la publication du programme de travail, la Commission a procédé à plusieurs constatations concernant le niveau adéquat de la protection des données. L'Argentine, Guernesey et l'Île de Man ont été considérés comme assurant un niveau adéquat de protection.

La Commission a également examiné le fonctionnement des décisions constatant le caractère adéquat de la protection des données qui ont été adoptées antérieurement. En 2004, un rapport des services de la Commission a été présenté concernant le fonctionnement de la sphère de sécurité (Safe Harbour), suivi d'une note d'information et d'un formulaire type pour le dépôt d'une plainte auprès du panel de protection des données. Ces travaux ont été suivis d'une grande conférence sur les transferts internationaux de données à caractère personnel organisée conjointement, en octobre 2006, par le groupe de travail et le ministère américain du commerce. Des constatations du niveau adéquat de protection des données ont également été faites pour la Suisse et le Canada.

b) Autres décisions prises au titre de l'article 26, paragraphe 4, afin d'offrir aux opérateurs économiques un choix plus vaste de clauses contractuelles types

La Commission a adopté une décision reconnaissant une nouvelle série de clauses contractuelles offrant des garanties adéquates pour le transfert de données à des responsables du traitement dans des pays tiers. Ces clauses avaient été proposées par un groupe d'associations professionnelles représentatives, dont la Chambre de commerce internationale. Les services de la Commission ont également présenté en 2006 un premier rapport concernant la mise en œuvre des décisions antérieures de la Commission sur les clauses contractuelles types.

c) Rôle joué par les règles d'entreprise contraignantes dans les garanties adéquates lors de transferts intra-groupes de données à caractère personnel

Après des travaux préparatoires en 2003 et en 2004, le groupe de travail a adopté deux documents clés. Le premier définit une procédure de coopération entre autorités nationales de contrôle en vue d'émettre des avis communs sur les garanties suffisantes offertes par les «règles d'entreprise contraignantes». Le second établit une liste de contrôle type à l'intention des responsables du traitement lorsqu'ils doivent introduire une demande d'approbation de règles de ce type afin de faire constater qu'elles offrent des garanties suffisantes.

d) Une interprétation plus uniforme de l'article 26, paragraphe 1, de la directive

Le groupe de travail a adopté un avis énonçant des lignes directrices sur le recours aux dérogations au principe de protection adéquate dans les pays tiers.

Action 8: Promotion des technologies renforçant la protection de la vie privée

Les travaux menés en 2003 et 2004 par la Commission et le groupe de travail ont débouché sur une communication relative aux technologies renforçant la protection de la vie privée que la Commission publiera prochainement et dans laquelle elle esquisse sa politique future en la matière.

Action 9: Promotion de l'autorégulation et des codes de conduite européens

Le groupe de travail a approuvé le Code de conduite de la Fédération européenne de marketing direct (FEDMA), qui marque une étape importante. Malheureusement, d'autres tentatives n'ont pas abouti à un code semblable, répondant à des critères de qualité comparables. Les partenaires sociaux européens n'ont pas réussi non plus à conclure un accord européen sur la protection des données à caractère personnel dans le cadre de l'emploi, et ce en dépit des progrès engrangés précédemment.

Action 10: Sensibilisation

Un sondage Eurobaromètre a été réalisé au niveau européen, afin de connaître l'opinion des citoyens et des entreprises en matière de protection de la vie privée. D'une manière générale, les gens s'intéressent aux questions touchant au respect de la vie privée, mais ils sont insuffisamment informés de l'existence de règles et de mécanismes protégeant leurs droits.

2. SITUATION ACTUELLE: APERÇU DE LA MISE EN ŒUVRE DE LA DIRECTIVE

La mise en application s'est améliorée.

Tous les États membres ont maintenant transposé la directive. Dans l'ensemble, la transposition nationale couvre toutes les dispositions essentielles en se conformant à la directive.

Les actions lancées dans le cadre du programme de travail se sont avérées positives et ont largement contribué à une meilleure application de la directive dans toute la Communauté. Les autorités nationales de contrôle chargées de la protection des données se sont pleinement engagées dans les travaux du groupe de travail, ce qui a eu un impact décisif.

Mais certains pays n'ont pas encore procédé à la mise en œuvre correcte de la directive.

Faisant suite aux travaux de préparation du premier rapport de la Commission en 2003, l'analyse approfondie, dans le cadre du dialogue structuré, de la législation nationale en matière de protection des données a éclairé la manière dont la directive a été transposée dans l'ensemble de la Communauté. Elle a clarifié une série de questions juridiques et a permis de lever certains doutes quant à la cohérence de certaines mesures et pratiques nationales avec les dispositions de la directive.

Le dialogue structuré a également montré que certains États membres n'avaient pas incorporé plusieurs dispositions importantes de la directive. Dans d'autres cas, la transposition ou la pratique s'était écartée de la directive ou avait dépassé la marge de manœuvre accordée aux États membres.

Une des préoccupations porte sur le respect de l'obligation de laisser les autorités nationales de contrôle chargées de la protection des données agir en toute indépendance et de les doter des pouvoirs et des ressources nécessaires à l'accomplissement de leurs tâches. Ces autorités constituent la pierre angulaire du système de protection conçu par la directive et le fait de ne pas leur accorder l'indépendance et les pouvoirs nécessaires a une incidence très négative sur le contrôle du respect de la législation en matière de protection des données.

Afin d'assurer une approche cohérente, la Commission mène une analyse comparée des situations dans lesquelles on soupçonne une transposition incorrecte ou incomplète. Certains États membres ont reconnu l'existence de lacunes dans leur législation et se sont engagés à les corriger, ce que la Commission encourage fermement. D'autres problèmes ont été mis en lumière par les plaintes introduites par des citoyens. Lorsqu'il s'avère que le droit communautaire a été enfreint, la Commission, en tant que gardienne des traités, lance une procédure formelle d'infraction à l'encontre de l'État membre concerné, conformément à l'article 226 du traité CE. Plusieurs procédures de ce type ont déjà été ouvertes.

La marge d'appréciation laissée par la directive explique certaines disparités.

La directive contient plusieurs dispositions dont la formulation est trop vague et qui, implicitement ou explicitement, laissent une marge d'appréciation aux États membres dans l'adoption de leur législation nationale. Du fait de cette marge d'appréciation, des disparités peuvent apparaître entre les législations nationales[6]. Elles ne sont pas plus importantes dans ce secteur que dans d'autres domaines de l'activité économique et sont la conséquence naturelle de la marge d'appréciation laissée par la directive.

Mais ces disparités ne constituent pas un réel problème pour le marché intérieur.

La Commission a commandé un rapport sur l'évaluation économique de la directive 95/46/CE sur la protection de données,[7] afin de mesurer l'impact économique de la directive sur les responsables du traitement. Une sélection de cas sont examinés et le rapport indique qu'en dépit de certains écarts, la mise en œuvre de la directive a entraîné peu de frais pour les sociétés.

---

6 Considérant 9 de la directive.

7 http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf.

Un plus grand degré de convergence serait certes souhaitable afin de promouvoir des initiatives positives telles que la simplification, l'autorégulation ou l'utilisation de règles d'entreprise contraignantes. Cependant, dans les plaintes reçues par la Commission, rien ne prouve que les disparités nationales dans les limites de la directive sont effectivement susceptibles d'empêcher le bon fonctionnement du marché intérieur ou de limiter la libre circulation des données pour des raisons liées à l'absence de protection ou à une protection inadéquate dans le pays d'origine ou de destination. De même, les contraintes dans le pays d'établissement ne faussent pas la concurrence entre les opérateurs privés. Les disparités nationales n'empêchent pas les sociétés de travailler ou de s'établir dans différents États membres. Elles ne remettent pas non plus en question l'engagement de l'Union européenne et de ses États membres en matière de protection des droits fondamentaux.

C'est pourquoi la directive atteint ses objectifs: garantir la libre circulation des données à caractère personnel au sein du marché intérieur, tout en assurant un niveau élevé de protection dans la Communauté.

Les règles sont pour l'essentiel appropriées.

La question est bien différente lorsqu'il s'agit de savoir si, au-delà de la réalisation de l'harmonisation, les solutions juridiques apportées par la directive sont à la hauteur des enjeux.

Certaines dispositions ont été critiquées. Il ressort des remarques formulées que la notification constitue une charge, mais qu'elle est très importante pour les personnes concernées comme mesure de transparence, qu'elle est un exercice de sensibilisation pour les responsables du traitement des données et qu'elle représente un outil de suivi pour les autorités. L'Internet ainsi que les nouvelles possibilités données aux personnes concernées d'interagir et d'accéder à des services fournis dans des pays tiers soulèvent des questions concernant les règles de détermination de la législation nationale applicable ou concernant les transferts de données vers des pays tiers, questions auxquelles la jurisprudence n'a répondu que partiellement[8]. Les dispositifs d'identification par radiofréquence (RFID) soulèvent des questions de fond quant à la portée des règles de protection des données et à la notion de données à caractère personnel. L'association à la reconnaissance automatique de données constituées par des sons ou des images impose une très grande prudence dans l'application des principes de la directive.

Un débat analogue a eu lieu au Conseil de l'Europe à propos de la pertinence des principes de la Convention 108 dans le monde d'aujourd'hui. De l'avis de tous, ces principes sont toujours valables et apportent des solutions satisfaisantes.

L'adaptation à l'évolution technologique.

La Commission estime que la directive est techniquement neutre, que ses principes et dispositions sont de portée suffisamment générale et que ses règles peuvent continuer à s'appliquer de manière satisfaisante aux technologies et situations nouvelles. Il peut néanmoins s'avérer nécessaire de traduire ces règles générales en lignes directrices ou en dispositions plus spécifiques afin de tenir compte des particularités de ces technologies.

---

[8] Arrêt du 6 novembre 2003, dans l'affaire C-101/01, Lindqvist.

En conséquence, la directive 2002/58/CE précise et complète la directive 95/46/CE en ce qui concerne le traitement de données à caractère personnel dans le secteur des communications électroniques, en assurant la libre circulation de ces données, ainsi que de l'équipement et des services en matière de communication électronique dans la Communauté. Cette directive est actuellement réexaminée à l'occasion du réexamen complet du cadre réglementaire sur les communications électroniques.

Le groupe de travail a fourni un important effort de réflexion dans le domaine technologique, par exemple sur les communications non sollicitées («pourriels»), les filtres pour le courrier électronique, le traitement des données relatives au trafic à des fins de facturation ou des données relatives à la localisation dans le cadre de la fourniture de services à valeur ajoutée. La technologie RFID a fait l'objet de plusieurs ateliers et d'une consultation publique lancée par les services de la Commission pour débattre des questions relatives à la vie privée et à la sécurité.

Examen des exigences imposées par l'intérêt public.

Dans la directive, l'articulation entre la protection des droits et libertés fondamentales des personnes et les besoins imposés par l'intérêt public est assurée par deux types de dispositions.

Le premier exclut du champ d'application de la directive un certain nombre de domaines, comme l'article 3 qui se réfère aux traitements ayant pour objet «la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal». La Cour de justice des Communautés européennes a précisé que le traitement ayant pour objet la sécurité publique et le traitement à des fins répressives ne relèvent pas du champ d'application de la directive[9]. Devant le besoin d'un ensemble harmonisé de règles de l'UE en matière de protection des données, la Commission a adopté une proposition relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[10] pour accompagner sa proposition relative à l'échange d'informations en vertu du principe de disponibilité[11]. Dans ce domaine, l'UE a conclu un accord international avec les États-Unis, afin de traiter la question de l'utilisation des données PNR des passagers dans la lutte contre la criminalité12.

Le second autorise les États membres à limiter les principes de protection des données sous certaines conditions, comme le prévoit l'article 13 «lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder [la liste d'intérêts publics importants qui suit]». Ces limitations peuvent tenir compte, par exemple, de la nécessité de lutter contre la criminalité ou de protéger la santé publique dans des situations de crise. D'autres dispositions de la directive prévoient des dérogations limitées. La Cour a précisé que les données initialement collectées à des «fins commerciales» ne peuvent être utilisées ensuite à d'autres fins d'intérêt public que dans le respect des conditions fixées audit article. En outre, les limites imposées au législateur national sont équivalentes à celles arrêtées à l'article 8 de la Convention européenne des droits de l'homme, et la jurisprudence de la Cour européenne des droits de l'homme revêt une

---

9 Arrêt du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 («PNR»).
10 COM(2005) 475 final du 4.10.2005.
11 COM(2005) 490 final du 12.10.2005.
12 JO L 298 du 27.10.2006, p. 29.

importance primordiale. [13]. Ce mécanisme, qui permet à un État membre d'apprécier ce qui constitue «une mesure nécessaire» et «un intérêt public important», est par nature une source de disparités entre les législations nationales.

Ces restrictions n'ont été harmonisées que dans un nombre restreint de secteurs, comme on l'a vu récemment avec la directive 2006/24/CE sur la conservation des données,[14] pour laquelle la Commission a annoncé son intention d'instituer un groupe d'experts chargé de débattre de problèmes comme la transposition de la directive dans la législation nationale.

Donner corps au droit fondamental.

La Commission s'est engagée à respecter dans toutes ses propositions la Charte des droits fondamentaux. En ce qui concerne le droit à la protection des données à caractère personnel prévu à l'article 8 de ladite Charte, la directive instaure une norme élevée et constitue une référence pour assurer la cohérence des dispositions sur le respect de la vie privée dans l'ensemble de la législation communautaire dans différents domaines.

3. L'AVENIR: PROCHAINES ÉTAPES

Tenant compte de cette situation, la Commission entend mener une politique présentant les caractéristiques suivantes.

La ratification du traité constitutionnel peut ouvrir de nouvelles perspectives.

Le traité constitutionnel aurait un énorme impact dans ce domaine. Il consacrerait, à l'article II-68, le droit à la protection des données à caractère personnel prévu à l'article 8 de la Charte des droits fondamentaux. Il créerait également à l'article I-51 une base juridique spécifique et autonome permettant à l'Union de légiférer en la matière et ouvrant la voie à l'adoption d'instruments applicables dans tous les secteurs. L'actuelle division en «piliers» et les limitations posées à l'article 3 de la directive ne feraient plus l'objet de débats. Toutefois, en attendant que la situation s'éclaircisse en ce qui concerne le processus de ratification du traité constitutionnel, la Commission a souligné la nécessité de recourir à des procédures plus efficaces dans l'espace de liberté, de sécurité et de justice en vertu des traités actuels[15].

La directive ne devrait pas être modifiée.

Pour les raisons exposées ci-dessus, la Commission estime que la directive relative à la protection des données constitue un cadre juridique général qui répond aux objectifs initiaux en constituant une garantie suffisante pour le bon fonctionnement du marché intérieur, tout en assurant un degré élevé de protection. La directive donne corps au droit fondamental de protection des données à caractère personnel; le respect de ses règles devrait rassurer les personnes quant à l'utilisation des informations les concernant, ce qui constitue une condition clé du développement de la cyberéconomie; elle est une référence pour les initiatives dans toute une série de domaines politiques; elle est techniquement neutre et continue à fournir des solutions concrètes et appropriées.

---

13 Arrêt du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01, Rechnungshof.

14 JO L 105 du 13.4.2006, p. 54.

15 COM(2006) 331 final du 28.6.2006.

En conséquence, la Commission n'envisage pas de soumettre une proposition législative visant à modifier la directive.

La Commission veillera à l'application correcte de ses dispositions au niveau national et international.

Certaines incohérences dans les législations nationales sont dues à une transposition incorrecte ou incomplète des dispositions de la directive. Sur la base des informations réunies dans le cadre du dialogue structuré avec les États membres, ainsi que de celles provenant des plaintes des citoyens, la Commission poursuivra son travail avec les États membres et, le cas échéant, lancera des procédures officielles d'infraction afin de garantir des conditions identiques à tous les États membres.

La Commission invite en outre instamment les États membres à veiller à la bonne mise en œuvre de la législation nationale adoptée en application de la directive. En même temps, elle suivra les développements dans les forums internationaux comme le Conseil de l'Europe, l'OCDE et les Nations Unies, et continuera d'y prendre part, afin que les engagements des États membres soient cohérents avec les obligations découlant de la directive.

La Commission préparera une communication interprétative pour certaines dispositions.

Les problèmes mis en évidence dans l'application de certaines dispositions de la directive, qui peuvent éventuellement donner lieu à des procédures formelles d'infraction, correspondent à une certaine compréhension de ces dispositions et de leur application correcte, en tenant compte de la jurisprudence, ainsi que des travaux d'interprétation menés par le groupe de travail.

Ces idées seront clairement présentées dans une communication interprétative.

La Commission encourage tous les acteurs concernés à mettre tout en œuvre pour réduire les disparités nationales.

Plusieurs actions seront menées dans cette optique.

– *Le programme de travail sera poursuivi.*

Les actions définies en 2003 en vue d'améliorer la mise en application de la directive étaient appropriées à cette époque et continuent de l'être.

Les activités énumérées dans le programme de travail seront poursuivies et l'association de tous les acteurs constitue une bonne base pour améliorer la mise en œuvre des principes de la directive.

– *Le groupe de travail devra améliorer sa contribution à l'harmonisation des pratiques.*

Rassemblant les autorités nationales de contrôle de la protection des données, le groupe de travail représente un élément clé pour assurer une application meilleure et plus cohérente. C'est ainsi que cette entité a pour mission «d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène». Le groupe de travail a déjà mené des travaux utiles en cherchant à obtenir une mise en œuvre uniforme au niveau national de certaines dispositions clés, telles que les flux transfrontières de données ou le concept de données à caractère personnel.

Afin de tirer pleinement parti de cette mission, les autorités de contrôle doivent également s'efforcer d'adapter leurs pratiques nationales afin de les aligner sur la ligne commune arrêtée au sein du groupe de travail.

Relever les défis des nouvelles technologies.

Les principes de la directive restent valables et ne devraient pas être modifiés. Toutefois, l'important développement des nouvelles technologies d'information et de communication requiert des orientations plus précises quant à la mise en pratique de ces principes. La sophistication accrue de la technologie permet la circulation rapide des informations dans le monde entier. Toutefois, le cas échéant, la technologie permet également de mieux protéger les données en les rendant plus faciles à contrôler et à rechercher. Les données pertinentes peuvent être identifiées plus rapidement et plus facilement. Lorsque le transfert de données n'est pas autorisé, la technologie permet d'isoler les données en question et de les protéger plus rapidement et plus efficacement que par le passé.

Le groupe de travail a un rôle très important à jouer. Il doit poursuivre le travail réalisé au sein de sa Task Force Internet et continuer à promouvoir une approche commune parmi les autorités nationales de contrôle, afin d'harmoniser l'application de la législation nationale, notamment en ce qui concerne les lois applicables et les flux transfrontières de données.

Lorsqu'une technologie particulière pose régulièrement problème sous l'angle du respect des principes relatifs à la protection des données et que son utilisation généralisée ou le risque d'intrusion pourraient justifier des mesures plus strictes, la Commission pourrait proposer une législation sectorielle au niveau de l'UE, afin que ces principes s'appliquent aux exigences spécifiques de la technologie en cause. C'est l'approche qui a été retenue dans la directive 2002/58/CE (directive sur la vie privée et les communications électroniques).

L'examen en cours de cette directive, ainsi que la communication sur l'identification par radiofréquence mentionnée ci-dessus peuvent être l'occasion de réfléchir à la nécessité de modifier cette directive ou d'adopter des règles spécifiques permettant d'apporter une solution aux problèmes de protection des données suscités par des technologies comme celle de l'Internet ou de la RFID.

Apporter une réponse cohérente aux exigences de l'intérêt public, notamment la sécurité.

Nous devons concilier deux exigences fondamentales: la lutte efficace contre les menaces qui pèsent sur la vie quotidienne des personnes en Europe, notamment en matière de sécurité et la protection des droits fondamentaux, y compris le droit à la protection des données. La quantité de données à caractère personnel collectées sur les personnes et le nombre d'activités impliquant la conservation et le stockage des traces de ces données sont considérables. Ces données ne peuvent être utilisées à d'autres fins que celles ayant justifié leur collecte à l'origine que pour autant que cette utilisation soit dûment autorisée. De telles mesures peuvent être nécessaires et justifiées, dans une société démocratique, par des raisons d'intérêt public comme la lutte contre le terrorisme et la criminalité organisée.

La Commission, en s'efforçant d'atteindre l'équilibre essentiel entre les mesures de sécurité et les mesures de protection des droits fondamentaux non négociables, veille au respect de la protection des données à caractère personnel, telle que garantie à l'article 8 de la Charte des droits fondamentaux. L'UE coopère également avec des partenaires extérieurs. À l'heure de la mondialisation, ceci est fondamental. En particulier, l'UE et les États-Unis entretiennent un dialogue transatlantique continu sur l'échange d'informations et la protection des données à caractère personnel à des fins d'application de la loi.

La Commission réexaminera l'application de la directive lorsque les mesures exposées dans la présente communication auront été menées à bien.