I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée

(2010/C 280/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, en particulier son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, en particulier ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ([1]),

vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement de données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques ([2]),

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et en particulier son article 41 ([3]),

ADOPTE L'AVIS SUIVANT:

I. INTRODUCTION

1. Les technologies de l'information et de la communication (TIC) ouvrent de nombreuses possibilités dans nos vies quotidiennes — notamment dans la façon dont nous travaillons, jouons, apprenons et entretenons des contacts avec nos semblables. Les TIC jouent un rôle majeur dans le monde actuel de l'information et dans la société en général.

2. L'Union européenne est un leader mondial dans ces technologies de pointe et souhaite le rester. C'est pour relever ce défi que la Commission européenne devrait adopter prochainement un nouveau programme numérique européen, dont la Commissaire Kroes a fait l'une de ses priorités ([4]).

3. Le CEPD reconnaît les bénéfices apportés par les TIC et considère que l'UE devrait faire de son mieux pour favoriser leur développement et la généralisation de leur utilisation. Il partage aussi entièrement la volonté des commissaires Kroes et Reding de placer les citoyens au cœur de ce nouvel environnement technologique ([5]). Les particuliers doivent pouvoir compter sur la capacité des TIC à garantir la sécurité de leurs informations et contrôler l'usage qui en est fait, et savoir que, dans cet espace numérique, leurs droits en matière de protection de la vie privée et de confidentialité des données seront respectés. Il est indispensable que ces droits soient pris en compte pour obtenir la confiance des consommateurs, et cette confiance est indispensable pour que les citoyens européens profitent des nouveaux services qui leurs sont proposés ([6]).

([1]) JO L 281 du 23.11.1995, p. 31.
([2]) JO L 201 du 31.7.2002, p. 37.
([3]) JO L 8 du 12.1.2001, p. 1.

([4]) Réponses au questionnaire du Parlement européen adressé à la commissaire Neelie Kroes dans le cadre des auditions préliminaires conduites par le Parlement européen en vue de la nomination des commissaires.

([5]) Réponses au questionnaire du Parlement européen adressé à la commissaire Neelie Kroes dans le cadre des auditions préliminaires conduites par le Parlement européen en vue de la nomination des commissaires; discours de la commissaire Viviane Reding «Un programme numérique européen répondant aux attentes des nouveaux consommateurs numériques» au Forum multipartite du BEUC (Bureau européen des unions de consommateurs) sur la protection de la vie privée des consommateurs et le marketing en ligne: «Tendances du marché et perspectives politiques», Bruxelles, le 12 novembre 2009.

([6]) Voir, par exemple, le rapport «La confiance accordée à la société de l'information» préparé par le conseil consultatif RISEPTIS (Recherche et innovation dans le domaine de la sécurité, la vie privée et la confiance accordée à la société de l'information). Disponible à l'adresse http://www.think-trust.eu/general/news-events/riseptis-report.html. Voir également: J. B Horrigan, *Broadband Adoption and Use in America*, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. L'UE a mis en place un cadre juridique solide pour la protection des données et de la vie privée, dont les principes restent valables à l'ère numérique. Néanmoins, elle ne doit pas sous-estimer l'ampleur de sa tâche. Les TIC soulèvent fréquemment de nouvelles questions qui ne sont pas prises en compte par le cadre réglementaire actuel. Des mesures doivent donc être prises pour assurer le respect des droits individuels prévus par le législateur communautaire et continuer à garantir aux citoyens européens une protection efficace dans ce nouvel environnement.

5. Le présent avis présente les mesures qui pourraient être promues ou adoptées par l'Union européenne pour protéger la vie privée et la protection des données des particuliers dans une société mondialisée toujours plus tournée vers la technologie. Elle expose les instruments législatifs et non législatifs qui pourraient être utiles à ces fins.

6. Après un aperçu des opportunités et des risques présentés par les TIC, l'avis examine la nécessité d'intégrer la protection des données et de la vie privée dès la conception de nouvelles technologies de l'information et de la communication (un principe dénommé «Privacy by Design» (respect de la vie privée dès la conception). Afin d'imposer l'application de ce principe à tous, l'avis analyse la façon dont il pourrait être intégré dans le cadre juridique relatif à la protection des données, ce qui pourrait être fait de deux manières différentes. La première consisterait à l'introduire dans la législation communautaire comme un principe général et contraignant, la seconde à l'intégrer dans certains aspects particuliers du secteur des TIC, en montrant comment une architecture et une conception techniques appropriées permettraient d'atténuer les risques spécifiques qui pèsent sur la protection des données et de la vie privée. Ces aspects particuliers sont la RFID (Radio Frequency Identification: identification par radiofréquence), les applications de socialisation sur internet et les applications de navigateurs. Enfin, l'avis formule des suggestions sur les autres outils et principes destinés à protéger la vie privée et les données relatives aux personnes dans le domaine des TIC.

7. Pour répondre à ces questions, l'avis reprend certains points soulevés par le groupe de travail «Article 29» dans sa contribution à la consultation publique sur l'avenir de la vie privée ([1]). Il s'appuie également sur certains avis précédents du contrôleur européen de la protection des données, ceux notamment du 25 juillet 2007 concernant la mise en œuvre de la directive 95/46/CE (ci-après «directive sur la protection des données») et du 20 décembre 2007 sur la RFID, ainsi que sur ses deux avis relatifs à la directive 2002/58/CE (ci-après directive «Vie privée et communications électroniques») ([2]).

II. LES TIC: NOUVELLES OPPORTUNITÉS, NOUVEAUX RISQUES

8. Les TIC ont été comparées à d'autres inventions importantes telles que l'électricité. S'il est trop tôt pour évaluer leur impact historique, dans les pays développés, le lien entre les TIC et la croissance économique est évident. Les TIC ont permis de créer des emplois, de réaliser des bénéfices économiques et ont contribué à l'amélioration générale du bien-être des citoyens. Leur impact dépasse le domaine purement économique puisqu'elles ont également joué un rôle important dans le développement de l'innovation et de la créativité.

9. En outre, les TIC ont transformé les modes de travail et d'interaction sociale. Par exemple, nous utilisons de plus en plus les TIC pour nos relations sociales et nos opérations économiques. Grâce aux nouvelles applications, nous pouvons utiliser un large éventail de TIC dans divers domaines tels que la santé (eSanté), les transports (eTransports), les affaires publiques (eGouvernement) ainsi que des systèmes interactifs innovants de divertissement et d'acquisition de connaissances.

10. C'est au regard de ces avancées que les institutions européennes se sont toutes engagées à soutenir les TIC et à tirer profit de cet outil indispensable pour améliorer la compétitivité des entreprises européennes et accélérer la reprise économique en Europe. Ainsi, au mois d'août 2009, la Commission a approuvé le rapport européen sur la compétitivité dans le domaine numérique ([3]) et a lancé une consultation publique sur les stratégies appropriées pour favoriser les TIC à l'avenir. Le 7 décembre 2009, le Conseil a remis sa contribution à la consultation «Stratégie post i2010 — Vers une société de la connaissance ouverte, compétitive et verte» ([4]). Le

([1]) Voir l'avis 168 du groupe de travail article 29 sur l'avenir de la protection de la vie privée, contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009.

([2]) Avis du 25 juillet 2007 du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1; avis du 20 décembre 2007 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique», document COM(2007) 96, JO C 101, 23.4.2008, p. 1; avis du 10 avril 2008 sur la proposition de directive modifiant, entre autres, la directive 2002/58/CE 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 C 181, 18.7.2008, p. 1; deuxième avis du 9 janvier 2009 relatif au réexamen de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

([3]) Rapport européen sur la compétitivité dans le domaine numérique — Principales réalisations de la stratégie i2010, 2005-2010 (SEC(2009) 1060).

([4]) Conclusions du Conseil «stratégie post-i2010 — Vers une société de la connaissance ouverte, compétitive et verte». (Document 17107/09 adopté le 18.12.2009).

Parlement européen a pour sa part récemment adopté un rapport destiné à aider la Commission à définir son Programme numérique [1].

11. Les opportunités et les bénéfices apportés par le développement des TIC s'accompagnent de nouveaux risques, notamment en ce qui concerne la vie privée et la protection des données personnelles des individus. Les TIC engendrent souvent une prolifération (qui passe inaperçu aux yeux des particuliers) du volume des informations collectées, triées, filtrées, transférées ou autrement conservées, ce qui multiplie les risques qui pèsent sur ces données.

12. Par exemple, les micropuces RFID remplacent les codes barres sur (certains) produits de consommation. En améliorant les flux d'information de la chaîne d'approvisionnement (et donc en réduisant le besoin de constituer des stocks de «sécurité», en fournissant des prévisions plus précises, etc.), ce nouveau système devrait soutenir les entreprises et les consommateurs. Toutefois, il accroît l'inquiétante possibilité de suivre les consommateurs à différentes fins et par différentes entités, via les articles personnels portant une micropuce d'identification.

13. Un autre exemple est constitué par l'«informatique dématérialisée» qui désigne principalement la mise à disposition sur internet d'applications hébergées destinées à des consommateurs ou des professionnels. Il peut s'agir de photothèques, calendriers, bases de données webmail et «customer» ainsi que de services professionnels plus complexes. Les bénéfices pour les entreprises et les personnes sont évidents: des coûts réduits et progressifs, mobilité géographique (accès à l'information partout dans le monde), automatisation (pas de nécessité d'employer du personnel dédié à l'informatique et de mettre les logiciels à jour) etc. Parallèlement, des risques de défaillance de la sécurité et de piratage informatique existent. Certains s'inquiètent aussi de perdre l'accès à leurs propres données et d'en perdre le contrôle.

14. Dans plusieurs domaines d'application des TIC, risques et bénéfices coexistent. Pour la santé par exemple, les services en ligne peuvent améliorer l'efficacité et l'accessibilité, réduire les coûts, et d'une manière générale, améliorer la qualité des services de soins. Cependant, certains doutes subsistent quant à la légitimité de l'utilisation secondaire des informations collectées dans ce cadre, et appellent à une analyse prudente des objectifs poursuivis lors de toute utilisation potentielle [2]. En outre, avec le recours accru aux systèmes de traitement électronique des dossiers de santé, différents problèmes de piratage se sont produits et ont fait scandale.

15. En somme, il est probable qu'un certain degré de risque résiduel persiste, même en évaluant et en appliquant les mesures appropriées. Le risque zéro ne peut exister. Néanmoins, comme nous le verrons plus en détails ci-après, des mesures peuvent et doivent être prises pour limiter les risques à un niveau acceptable.

III. «PRIVACY BY DESIGN», RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION: UN OUTIL CLÉ DE LA CONFIANCE DES CITOYENS À L'ÉGARD DES TIC

16. Les bénéfices potentiels des TIC ne peuvent être appréciés dans la pratique que si les TIC suscitent la confiance des utilisateurs par leurs caractéristiques et les avantages qui leurs sont propres. Cette confiance ne peut s'établir que si les TIC s'avèrent fiables et sûres, si les utilisateurs peuvent les contrôler, et enfin si elles garantissent la protection de leurs données à caractère personnel et de leur vie privée.

17. Les risques et défaillances les plus courants (tels que ceux mentionnés plus haut) ébranlent la confiance des utilisateurs à l'égard de la société de l'information, surtout lorsque des données à caractère personnel ou liées à la vie privée des personnes sont mal employées ou utilisées de manière abusive. Cela pourrait sérieusement menacer le développement des TIC et de ses avantages.

18. Cependant, l'élimination, l'exclusion ou le refus d'utiliser ou d'encourager les TIC ne sauraient être la solution pour éliminer les risques qui pèsent sur la vie privée et les données à caractère personnel. Cette option ne serait d'ailleurs ni réalisable ni réaliste car elle empêcherait les citoyens d'apprécier les bénéfices des TIC et limiterait sérieusement l'étendue de leurs avantages.

19. Le CEPD estime qu'il serait nettement plus avantageux de concevoir et de développer les TIC de manière à protéger la vie privée et la confidentialité des données à caractère personnel. C'est pourquoi ces deux aspects doivent être intégrés dans le cycle de vie entier de ce type de technologie, du stade précoce de sa conception jusqu'à sa commercialisation, son utilisation et sa mise au rebus. Ce concept dénommé «Privacy by design» (PbD) en anglais et «respect de la vie privée dès la conception» en français sera développé plus loin.

20. Le principe de «respect de la vie privée dès la conception» peut s'appliquer à différentes actions, en fonction du dossier ou de l'application concernés. Il peut s'agir, selon les cas, d'éliminer/réduire le nombre de données à caractère personnel traitées, ou d'éviter tout traitement non nécessaire et/ou non souhaité. Il peut aussi s'agir de proposer aux utilisateurs des outils leur permettant d'améliorer le contrôle exercé sur les données à caractère personnel les concernant. Ces mesures devront être envisagées lorsque des normes et/ou des bonnes pratiques auront été définies dans ce domaine. Elles pourront aussi être incorporées dans l'architecture des systèmes

[1] Rapport sur l'élaboration d'un nouvel agenda numérique pour l'Europe: de i2010 à digital.eu [2009/2225 (INI)], adopté le 18.3.2010.

[2] Par exemple, des informations sanitaires collectées en vue de traitements médicaux ne sauraient être utilisées ou vendues sans une extrême prudence pour sélectionner un site pour une clinique satellite, établir un centre de chirurgie ambulatoire, ni d'aucune autre façon pour planifier des activités futures ayant des implications financières.

d'information et de communication ou dans l'organisation structurelle des entités qui procèdent au traitement de données à caractère personnel.

III.1. **Le principe du respect de la vie privée dès la conception: conséquences de son application dans différents environnements TIC**

21. La nécessité du principe de respect de la vie privée dès la conception existe dans différents environnements TIC. Le secteur de la santé par exemple, dépend de plus en plus d'infrastructures TIC souvent fondées sur une unité centrale de conservation des informations médicales des patients. Pour pouvoir appliquer le principe de respect de la vie privée dès la conception au secteur de la santé, il serait nécessaire d'évaluer différentes mesures et leur adéquation, comme par exemple, limiter le volume des données stockées de manière centralisée ou contrôler les données au moyen d'un répertoire, en utilisant des outils de cryptage, en attribuant des droits d'accès aux seuls intervenant ayant réellement besoin d'accéder aux données («besoin d'en connaître»), ou en rendant les données anonymes dès qu'elles ne sont plus nécessaires, etc.

22. De même, les moyens de transport sont de plus en plus fréquemment fournis avec des applications TIC avancées préinstallées qui entrent en interaction avec le véhicule et son environnement à des fins différentes et dans le cadre de fonctions distinctes. Par exemple, les voitures sont de plus en plus souvent équipées de nouvelles fonctionnalités TIC (GPS, GSM, réseau de détecteurs, etc.) qui informent en temps réel, non seulement sur leur localisation mais aussi sur leur état technique. Ces outils pourraient être utilisés par exemple pour remplacer les péages routiers par un paiement forfaitaire basé sur la fréquence d'utilisation des routes. L'intégration du principe de respect de la vie privée dès la conception dans l'architecture de ces systèmes devrait permettre de limiter au maximum le volume des données à caractère personnel traitées et transférées par la suite ([1]). Pour appliquer ce principe, il serait préférable d'opter pour des architectures décentralisées ou semi-décentralisées limitant la communication des données de localisation à un point central, plutôt que pour des architectures centralisées.

23. Les exemples précédents montrent que l'intégration du respect de la vie privée dès la conception dans les technologies de l'information et de la communication permettrait de réduire de manière significative les risques pesant sur la protection de la vie privée et la confidentialité des données.

III.2. **Le recours aux TIC appliquant le principe de respect de la vie privée dès la conception est encore trop rare**

24. Il serait nécessaire de déterminer si les opérateurs économiques, les fabricants/fournisseurs de TIC et les responsables du traitement des données souhaitent promouvoir et mettre en œuvre le principe de respect de la vie privée dès la conception. Il conviendrait également d'évaluer la demande des utilisateurs à cet égard.

25. En 2007, la Commission a publié une communication appelant les entreprises à utiliser leur capacité à innover pour créer et mettre en œuvre des PET (Privacy enhancing technologies: technologies renforçant la protection de la vie privée) afin d'améliorer la protection de la vie privée et la confidentialité des données à caractère personnel dès le début du cycle de développement des technologies ([2]).

26. Cependant, les informations collectées montrent que ni les fabricants de dispositifs TIC ni les responsables du traitement des données (du secteur privé comme du secteur public) ne sont à ce jour parvenus à mettre en œuvre ou à distribuer de manière systématique le principe de respect de la vie privée dès la conception. Différents motifs sont évoqués, dont l'absence d'incitations économiques ou de soutien institutionnel, une demande insuffisante etc ([3]).

27. Dans le même temps, la demande de technologies prenant en compte la vie privée dès la conception s'est avérée plutôt faible du côté des utilisateurs. Les utilisateurs de produits et services basés sur les TIC peuvent supposer à juste titre que leur vie privée et les données à caractère personnel les concernant sont de facto protégées, alors que souvent, ce n'est pas le cas. Parfois, ils ne sont tout simplement pas capables de prendre les mesures de sécurité qui permettraient de protéger leurs propres données ou celles qui concernent d'autres personnes. Cela résulte souvent du fait que les utilisateurs ne connaissent pas l'ensemble, voire une partie seulement, des risques encourus. Par exemple, les jeunes méconnaissent la plupart du temps les risques concernant leur vie privée lorsqu'ils affichent des informations personnelles sur les réseaux sociaux, et ignorent souvent les paramètres de confidentialité. D'autres utilisateurs connaissent ces risques mais n'ont pas le savoir-faire technique nécessaire pour mettre en place une véritable protection qui permettrait par exemple de protéger leur connexion internet, ou ne savent pas modifier les paramètres de leur navigateur afin de limiter les actions de «profiling» (surveillance des sites consultés sur internet).

28. Toutefois, les risques qui pèsent sur la protection de la vie privée et des données qui les concernent sont bien réels. Lorsque la protection de la vie privée et des données n'est pas prise en compte dès le départ, il est par la suite

([1]) Voir l'avis du contrôleur européen de la protection des données du 22 juillet 2009 sur la communication de la Commission relative au «Plan d'action pour le déploiement de systèmes de transport intelligents en Europe» et la proposition de directive du Parlement européen et du Conseil établissant un «Cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport»: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Communication du 2 mai 2007 [COM(2007) 228 final] de la Commission au Parlement européen et au Conseil: «Promouvoir la protection des données par les technologies renforçant la protection de la vie privée (PETs)».

([3]) Étude sur les avantages économiques des technologies renforçant la protection de la vie privée (PET) (jls/2008/D4/036).

souvent trop tard et trop coûteux pour rétablir le système et réparer les dégâts subis. Le nombre croissant de failles de sécurité constatées au cours des dernières années illustre parfaitement ce problème et renforce la nécessité de mettre en œuvre des systèmes fondés sur le principe de respect de la vie privée dès la conception.

29. Ceci indique clairement que les fabricants et les distributeurs de TIC conçues pour le traitement de données à caractère personnel devraient partager avec les responsables du traitement la responsabilité de concevoir des TIC munies d'outils intégrés de protection des données et de la vie privée, avec cette conséquence que les TIC devraient très souvent être conçues avec un paramétrage PhD.

30. Dans ce contexte, nous devons réfléchir aux mesures que les décideurs politiques pourraient proposer pour promouvoir le principe de respect de la vie privée dès la conception dans le développement des TIC. Dans un premier temps, il convient de déterminer si le cadre législatif actuel sur la protection des données est apte à garantir la mise en œuvre du principe de respect de la vie privée dès la conception par les responsables du traitement des données et par les fabricants/développeurs. Ensuite, il convient de déterminer les mesures à prendre dans le cadre du programme numérique européen pour susciter la confiance des consommateurs à l'égard des TIC.

IV. **INTÉGRER LE PRINCIPE DE RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION DANS LES TEXTES LÉGISLATIFS ET LES POLITIQUES COMMUNAUTAIRES**

IV.1. **Le cadre juridique actuel relatif à la protection des données et de la vie privée**

31. L'UE s'est dotée d'une solide protection des données et de la vie privée en adoptant les directives 95/46/CE [1] et 2002/58/CE [2], d'une part, et la jurisprudence de la Cour européenne des droits de l'homme [3] et de la Cour de justice, d'autre part.

32. La directive sur la protection des données à caractère personnel s'applique à «tout traitement ou ensemble de traitements de données à caractère personnel» (collecte, conservation, communication, etc.). Elle impose le respect de certains principes et de certaines obligations aux personnes chargées du traitement de ces données («les responsables du traitement»). Elle prévoit des droits individuels tels que le droit d'accéder à ses propres informations personnelles. La directive «Vie privée et communications électroniques» traite en particulier de la protection de la vie privée dans le secteur des communications électroniques [4].

33. La directive en vigueur sur la protection des données à caractère personnel n'exige pas explicitement d'instaurer le principe de respect de la vie privée dès la conception. Elle contient néanmoins des dispositions qui, dans certaines circonstances, pourraient indirectement exiger sa mise en œuvre. C'est notamment le cas de l'article 17 qui impose aux responsables du traitement des données de «mettre en œuvre les mesures techniques et d'organisation appropriées» pour prévenir tout traitement illicite [5]. Le principe de respect de la vie privée dès la conception est donc partiellement couvert. En outre, les dispositions de la directive s'adressent principalement aux responsables du traitement des données et concernent avant tout leurs opérations de traitement de données à caractère personnel. Elles ne prévoient pas explicitement la conformité des TIC avec les exigences relatives à la protection de la vie privée et des données, ce qui impliquerait aussi les concepteurs et les fabricants de TIC, ainsi que les activités menées au stade de la normalisation.

34. La directive «Vie privée et communications électroniques» est plus explicite à cet égard. Son article 14, paragraphe 3, dispose: «Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel, conformément à la directive 1999/5/CE et à la décision 87/95/CEE du Conseil du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications». Néanmoins, cette disposition n'a jamais été appliquée [6].

35. Si les dispositions des deux directives sont utiles à la *promotion* du principe de protection de la vie privée dès la conception, en pratique, elles n'ont pas suffi à *garantir* l'intégration de mesures de protection de la vie privée dans les TIC.

36. Il ressort de cette situation que le droit n'impose pas assez précisément une conception des TIC conforme au principe de respect de la vie privée dès la conception. Par ailleurs,

(1) Directive 95/46/CE du Parlement européen et du Conseil («directive sur la protection des données»).

(2) Directive 2002/58/CE du Parlement européen et du Conseil (Directive «Vie privée et communications électroniques»).

(3) Interprétant les principaux éléments et conditions établis par l'article 8 de la Convention européenne pour la protection des droits humains et des libertés fondamentales (ECHR) adoptée à Rome le 4 novembre 1950, tels qu'ils s'appliquent.

(4) Le traité de Lisbonne a renforcé cette protection en considérant le respect de la vie privée et la protection des données à caractère personnel comme des droits fondamentaux (articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne). Cette charte est entrée en vigueur avec le traité de Lisbonne.

(5) Article 17: «Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite». Le considérant 45 complète l'article 17: «Considérant que la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en œuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé».

(6) La Commission a annoncé son intention de mettre à jour la directive 1999/5/CE à la fin de l'année 2010.

les autorités chargées de la protection des données ne disposent pas des prérogatives nécessaires pour garantir cette intégration du principe de respect de la vie privée dès la conception. Il s'ensuit une certaine inefficacité. Ainsi par exemple, les autorités chargées de la protection des données peuvent être en mesure d'imposer une sanction en cas d'absence de réponse à une demande d'accès émanant d'un citoyen et sont habilitées à exiger la mise en œuvre de certaines mesures visant à prévenir le traitement illicite de données. Il n'est cependant pas toujours évident de savoir si ces autorités ont la faculté d'exiger qu'un système soit conçu de manière à faciliter les droits de protection des données à caractère personnel ([1]). Les textes juridiques actuels ne précisent pas, par exemple, s'il serait possible d'exiger qu'une architecture-système soit conçue de manière à faciliter la réponse des entreprises aux demandes d'accès formulées par les particuliers, de sorte que le traitement de ces demandes puisse être automatisé et plus rapide. Nous savons en outre qu'une fois qu'une technologie a été mise au point et distribuée, il est difficile de la modifier; les diverses tentatives dans ce sens risquent bien d'aboutir à un patchwork de solutions qui non seulement ne fonctionneront jamais correctement, mais auront aussi un coût élevé.

37. Le CEPD recommande donc, à l'instar du groupe de travail Article 29, ([2]) de prévoir, dans le cadre législatif actuel, la possibilité d'adhérer plus précisément au principe de respect de la vie privée dès la conception.

IV.2. **L'intégration du principe de «respect de la vie privée dès la conception» à différents niveaux**

38. À la lumière de ce qui précède, le CEPD recommande quatre mesures à la Commission:

a) Proposer d'intégrer une disposition générale sur le respect de la vie privée dès la conception dans les textes juridiques relatifs à la protection des données.

b) Formuler cette disposition générale sous forme de dispositions spécifiques lorsque différents instruments juridiques sont proposés, dans différents secteurs. Ces dispositions spécifiques pourraient déjà être intégrées dans l'appareil juridique, sur la base de l'article 17 de la directive sur la protection des données à caractère personnel (et d'autres textes législatifs).

c) Inclure le principe de respect de la vie privée dès la conception dans le Programme numérique européen, en tant que principe directeur.

d) Introduire le principe de respect de la vie privée dès la conception en tant que principe dans d'autres initiatives communautaires (principalement des initiatives non législatives).

Une disposition générale sur le respect de la vie privée dès la conception

39. Le CEPD propose d'intégrer le principe de respect de la vie privée dès la conception dans le cadre réglementaire actuel relatif à la protection des données, de manière explicite et non équivoque. Ceci permettrait de renforcer le principe de respect de la vie privée dès la conception, de le rendre plus explicite et d'imposer sa mise en œuvre effective, et donnerait aux autorités répressives une plus grande légitimité pour exiger qu'il soit de facto appliqué. Ceci semble particulièrement nécessaire au regard des faits précités: le principe joue non seulement un rôle important pour susciter la confiance des utilisateurs, mais aussi pour inciter les parties prenantes à mettre en œuvre le principe de respect de la vie privée dès la conception et améliorer les garanties prévues par le cadre juridique en vigueur.

40. Cette proposition s'inspire de la recommandation formulée par le groupe de travail article 29 visant à faire du principe de «respect de la vie privée dès la conception» un principe général au sein du cadre législatif relatif à la protection des données, en l'intégrant notamment dans la directive sur la protection des données. Le groupe de travail article 29 a indiqué: «Ce principe devrait être contraignant pour les concepteurs et producteurs de technologies ainsi que pour les responsables du traitement des données chargés de l'achat et de l'utilisation des TIC. Ils devraient avoir l'obligation de prendre en compte la protection technologique des données dès la phase de planification des procédures et des systèmes technologiques d'information. Les fournisseurs de tels systèmes ou services et les responsables du traitement des données devraient démontrer qu'ils ont pris toutes les mesures requises pour remplir ces obligations».

41. Le CEPD salue également le soutien que la commissaire Viviane Reding a manifesté à l'égard du principe de respect de la vie privée dès la conception lorsqu'elle a annoncé le réexamen de la directive sur la protection des données ([3]).

42. Examinons le contenu de cette directive. Tout d'abord, un principe général de respect de la vie privée dès la conception se doit d'être neutre sur le plan technologique. Il ne doit pas avoir pour fin de réglementer la technologie, c'est-à-dire qu'il n'est pas supposé prescrire de solution technique spécifique. Il doit au contraire favoriser l'intégration des principes relatifs à la protection de la vie

([1]) Voir le rapport du *UK Information Commissioner's Office* (ICO) intitulé: «Privacy by Design», publié en novembre 2008.

([2]) Voir l'avis n° 168 du groupe de travail article 29 sur l'avenir de la protection de la vie privée — Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009.

([3]) Le principe de respect de la vie privée dès la conception est intéressant pour les citoyens et les entreprises. Sa mise en œuvre aboutira à une protection accrue des personnes et suscitera leur confiance à l'égard des nouveaux produits et services proposés, ce qui sera également profitable pour l'économie. Si nous disposons déjà d'exemples encourageants, nous avons encore beaucoup à faire. Discours-programme prononcé lors de la «Journée de la protection des données», le 28 janvier 2010, Parlement européen, Bruxelles.

privée et des données existants dans les systèmes et solutions d'information et de communication. Les parties prenantes, les fabricants, les responsables du traitement des données et les autorités chargées de la protection des données devraient être en mesure d'interpréter le principe dans chaque situation particulière. Deuxièmement, le respect du principe devrait être obligatoire à différents stades, de l'élaboration de normes et d'une architecture à leur mise en place par le responsable du traitement des données.

Les dispositions des instruments juridiques spécifiques

43. Les textes réglementaires actuels et à venir doivent intégrer le principe de respect de la vie privée dès la conception en tenant compte du cadre législatif en place et des dispositions générales précitées, une fois qu'elles auront été adoptées. Si l'on se réfère aux initiatives actuelles, par exemple dans le domaine des systèmes de transport intelligents, on peut supposer que la Commission assumera la responsabilité spécifique initiale de définir des mesures, de prendre des initiatives de normalisation et d'adopter des procédures et des bonnes pratiques dans ce domaine. Le principe de respect de la vie privée dès la conception sera un principe directeur au cours de ce processus.

44. Le CEPD remarque ensuite que le principe de respect de la vie privée dès la conception joue également un rôle particulier dans le domaine des libertés, de la sécurité et de la justice, notamment en ce qui concerne les objectifs de la stratégie de gestion de l'information tels qu'énoncés dans le programme de Stockholm ([1]). Dans son avis relatif au programme de Stockholm, le CEPD a souligné que l'architecture des échanges d'informations devrait reposer sur le principe de respect de la vie privée dès la conception ([2]): «(…) ce qui signifie plus concrètement que les systèmes d'information élaborés à des fins de sécurité publique devraient toujours être construits conformément au principe de la "prise en compte du respect de la vie privée dès la conception"».

45. L'avis du groupe de travail article 29 sur l'avenir de la protection de la vie privée ([3]) insiste encore plus précisément sur le fait que dans le domaine des libertés, de la sécurité et de la justice (dans lequel les autorités publiques jouent le rôle principal et dans lequel le renforcement de la surveillance a un impact direct sur le droit fondamental au respect de la vie privée et de la confidentialité des données à caractère personnel), le principe de respect de la vie privée dès la conception devrait être obligatoirement appliqué. En l'introduisant dans les systèmes d'information, les gouvernements montreront l'exemple.

Le respect de la vie privée dès la conception: un principe directeur du programme numérique européen

46. Les technologies de l'information et de la communication sont de plus en plus complexes et comportent des risques accrus pour la protection de la vie privée et la confidentialité des données. En général, les informations au format numérique sont plus faciles à consulter, copier et transmettre mais aussi exposées à des risques bien plus importants que les informations sur papier. À mesure que nous évoluerons vers des réseaux d'objets interconnectés, les risques augmenteront. Plus les risques pesant sur la protection de la vie privée et des données seront élevés, plus la demande de garanties dans ce domaine sera élevée. La mise en œuvre du principe de respect de la vie privée dès la conception est dès lors d'autant plus justifiée dans le secteur des TIC. En outre, comme nous l'avons déjà mentionné, il est indispensable que les citoyens fassent confiance aux TIC pour adopter les nouveaux services qui leurs sont proposés. La protection de la vie privée et des données est un élément clé pour obtenir cette confiance.

47. Il découle de ce qui précède que toute stratégie de développement des TIC devra tenir compte de la nécessité d'intégrer un élément inhérent de protection de la vie privée et des données, c'est-à-dire le principe du respect de la vie privée dès la conception.

48. Le programme numérique européen devrait donc souscrire sans réserve à ce principe car il s'agit d'un élément indispensable pour obtenir la confiance des citoyens à l'égard des TIC et des services en ligne. Il devrait aussi reconnaître que vie privée et confiance vont de pair, et que le respect de la vie privée dès la conception est un principe directeur pour le développement d'un secteur TIC digne de confiance.

Le principe du respect de la vie privée dès la conception au sein des autres initiatives de l'UE

49. La Commission devrait adopter le principe comme principe directeur lors de la mise en œuvre de ses politiques, activités et initiatives dans certains secteurs spécifiques des TIC, notamment: eSanté, eApprovisionnement, eSécurité sociale, eLearning, etc. Nombre de ces initiatives figureront dans le programme numérique européen.

50. Cela signifie par exemple que les initiatives visant à accroître l'efficacité et la modernité des applications publiques permettant aux citoyens d'entrer en contact avec les différentes administrations devront intégrer le principe et s'y conformer. Il en va de même pour les politiques et les activités de la Commission dans plusieurs domaines: rapidité de l'internet, contenus numériques, amélioration des communications fixes et sans fil, et transmission de données.

([1]) Programme de Stockholm pour une Europe ouverte et sûre qui sert et protège les citoyens, adopté par le Conseil de l'UE en décembre 2009.

([2]) Avis du 10 juillet 2009 sur la communication de la Commission au Parlement européen et au Conseil sur un espace de liberté, de sécurité et de justice au service des citoyens, JO C 276, 17.11.2009, p. 8, point 60.

([3]) Voir l'avis n° 168 du groupe de travail article 29 sur l'avenir de la protection de la vie privée — Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, 1er décembre 2009.

51. Une telle approche inclut les systèmes informatiques de grande envergure tels que SIS et VIS gérés par la Commission, ainsi que les projets pour lesquels la responsabilité de la Commission se limite au développement et à la maintenance de l'infrastructure commune d'un tel système (par exemple ECRIS, le système européen d'information sur les casiers judiciaires).

52. La manière précise dont le principe de respect de la vie privée dès la conception sera développé dépendra de chaque secteur et de chaque situation particulière. Par exemple, lorsque les initiatives de la Commission seront accompagnées d'une proposition de loi concernant un secteur TIC spécifique, il sera souvent judicieux d'y faire figurer une mention spéciale indiquant la possibilité d'appliquer le principe de respect de la vie privée dès la conception de l'application/du système TIC concerné. Si un plan d'action est envisagé dans un domaine spécifique, il devra systématiquement garantir que le cadre légal est respecté et, plus précisément, que la technologie TIC concernée a été conçue en tenant compte du principe de respect de la vie privée dès la conception.

53. En ce qui concerne la recherche, le septième programme-cadre et les programmes suivants devraient servir de support à des projets qui visent à rechercher les normes, les technologies et l'architecture TIC les plus utiles pour la protection de la vie privée et, plus précisément, pour l'application du principe de respect de la vie privée dès la conception. En outre, le principe devrait être pris en compte dans des projets TIC plus larges prévoyant le traitement de données à caractère personnel.

Domaines particuliers

54. Dans certains cas, en raison de risques particuliers pesant sur la vie privée et la confidentialité des données, ou en raison d'autres éléments (réticence des entreprises à fournir des produits respectant la vie privée dès la conception, demande des consommateurs, etc.), il peut s'avérer nécessaire de définir des mesures de respect de la vie privée dès la conception plus explicites et spécifiques qui seront alors intégrées dans un type donné de produit/technologie TIC, que ce soit ou non dans un cadre législatif.

55. Le CEPD a identifié trois domaines, à savoir la RFID, les réseaux sociaux et les applications de navigation, que la Commission devrait examiner attentivement avec les mesures d'intervention directe précédemment exposées. Ces trois domaines sont présentés plus en détails ci-dessous.

V. **L'IDENTIFICATION PAR RADIOFRÉQUENCE (RFID)**

56. Les micropuces RFID peuvent être insérées dans des objets ou placées sur des animaux et des personnes. Elles peuvent être utilisées pour recueillir et conserver des données à caractère personnel telles que des dossiers médicaux, pour suivre les mouvements des personnes ou établir leur profil comportemental, à différentes fins. Ceci peut être réalisé sans que la personne concernée n'en soit consciente ([1]).

57. Des garanties efficaces relatives à la protection des données, de la vie privée et à l'ensemble des dimensions éthiques associées sont cruciales pour susciter la confiance du public à l'égard de la RFID et du futur internet des objets. Ce n'est que dans ces conditions que la technologie pourra apporter ses nombreux avantages économiques et sociaux.

V.1. **Les failles du cadre juridique actuel relatif à la protection des données**

58. La directive sur la protection des données et la directive «Vie privée et communications électroniques» s'appliquent à la collecte de données par l'intermédiaire d'applications RFID ([2]). Elles imposent notamment la mise en œuvre de garanties appropriées en matière de protection de la vie privée avant d'exploiter les applications RFID ([3]).

59. Néanmoins, ce cadre juridique ne répond pas entièrement aux questions que soulève cette technologie en matière de protection des données et de la vie privée. En effet, les directives ne sont pas suffisamment précises en ce qui

([1]) Le sigle RFID désigne l'identification par radiofréquence. Les principaux composants d'une application technologique *ou* d'une infrastructure RFID sont le *tag* (une micropuce), le lecteur et l'application liée aux micropuces et au lecteur par l'intermédiaire d'un *middleware* (logiciel médiateur), qui traitent les données produites. La micropuce contient un circuit électronique qui stocke les données et une antenne qui communique les données via des ondes radio. Le lecteur possède une antenne et un démodulateur qui transforme en données numériques les informations analogiques qui entrent par le biais du lien radio. Les informations ainsi transformées peuvent être envoyées via des réseaux à des bases de données et des serveurs, puis être traitées par un ordinateur.

([2]) L'article 3 de la directive «Vie privée et communications électroniques» fait référence à la technologie RFID: «La présente directive 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 dans la Communauté, y compris les réseaux de communication publics qui prennent en charge les dispositifs de collecte de données et d'identification». Le considérant 56 le complète ainsi: «Le progrès technologique permet le développement de nouvelles applications fondées sur des dispositifs de collecte de données et d'identification qui peuvent être des dispositifs sans contact utilisant les fréquences radio. Par exemple, les dispositifs d'identification par radiofréquence (RFID) utilisent les fréquences radio pour capturer des données à partir de tags identifiés de manière individuelle, puis les transférer sur les réseaux de communication existants. La généralisation de l'utilisation de ces technologies peut apporter des avantages économiques et sociaux considérables, et favoriser ainsi le marché intérieur, dès lors que les citoyens en adoptent le fonctionnement. Pour y parvenir, il faut s'assurer que l'ensemble des droits fondamentaux des individus, y compris le droit à la vie privée et à la protection de ses propres données, soient protégés. Lorsque ces dispositifs sont connectés à des réseaux de communications électroniques disponibles pour le public ou utilisent des services de communication électronique comme une infrastructure de base, les disposition pertinentes de la directive 2002/58/CE (directive "Vie privée et communications électroniques") doivent s'appliquer, ainsi que les dispositions relatives à la sécurité, au trafic, aux données de localisation et à la confidentialité».

([3]) Ainsi par exemple, l'article 17 de la directive sur la protection des données impose la mise en œuvre de «mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite (…) ou la diffusion non autorisée».

concerne le genre de garanties qui devraient être mises en œuvre avec les applications RFID. Les règles existantes doivent être complétées par de nouvelles dispositions qui imposeraient des garanties spécifiques, rendant notamment obligatoire le fait d'intégrer des solutions technologiques (privacy by design) dans la technologie RFID. Ceci concerne les micropuces d'identification qui stockent des informations personnelles: elles devraient être dotées de «kill commands» (commandes permettant de terminer un processus) et de fonctions de cryptographie pour les micropuces qui recueillent certains types d'informations.

V.2. **L'auto-régulation comme première étape**

60. En mars 2007, la Commission a adopté une communication ([1]) qui reconnaissait, entre autres, la nécessité d'élaborer des lignes directrices détaillées sur la mise en œuvre concrète de la RFID, et l'opportunité d'adopter des critères de conception destinés à éviter les risques pesant sur la vie privée et la sécurité des données.

61. Pour atteindre ces objectifs, la Commission a adopté en mai 2009 une recommandation sur «la mise en œuvre des principes de protection de la vie privée et des données personnelles dans les applications fondées sur la RFID» ([2]). Dans le commerce de détail, elle demande que les micropuces soient désactivées sur le point de vente, sauf si les consommateurs ne le souhaitent pas. Ceci s'appliquera sauf si une évaluation de l'impact sur la protection de la vie privée et des données montre que les micropuces d'identification ne représentent pas une menace potentielle pour la vie privée et les données à caractère personnel, auquel cas les applications RFID resteront opérationnelles après le point de vente (excepté si les personnes concernées s'y opposent, ce qui peut être fait gratuitement).

62. Les CEPD est favorable à l'approche d'auto-régulation préconisée par la Commission. Cependant, comme nous le verrons plus en détail ci-après, l'auto-régulation pourrait ne pas apporter les résultats souhaités; le CEPD recommande donc à la Commission de se tenir prête à adopter des mesures alternatives.

V.3. **Domaines particuliers et éventuelles mesures complémentaires à prendre en cas d'échec de l'auto-régulation**

63. Le CEPD se demande si les organisations qui exploitent des applications RFID dans le secteur du détail ne vont pas négliger la possibilité que ces micropuces donnent lieu à une surveillance non souhaitée par des tiers. Cette surveillance pourrait révéler des données à caractère personnel stockées dans la micropuce (le cas échéant) mais pourrait aussi permettre à un tiers de suivre ou reconnaître une personne à long terme, simplement en utilisant les identificateurs uniques contenus dans une ou plusieurs micropuces portées par un individu dans des lieux pouvant même aller au-delà du périmètre opérationnel de l'application RFID. Il est également préoccupé par le fait que les opérateurs d'applications RFID pourraient parfois être tentés, à tort, de laisser la micropuce fonctionner après le point de vente.

64. Si cela se produisait, il serait trop tard pour limiter les risques pesant sur la protection des données à caractère personnel et de la vie privée, celles-ci pouvant avoir été déjà affectées. De plus, compte tenu de la nature de l'auto-régulation, les autorités nationales répressives pourraient se trouver dans une position de faiblesse au moment de demander aux organisations opérant des applications RFID de mettre en œuvre des mesures de respect de la vie privée dès la conception.

65. Dès lors, le CEPD recommande à la Commission de se préparer à faire des propositions de loi pour réglementer les principaux aspects de l'utilisation de dispositifs RFID en cas d'échec de la mise en œuvre effective du cadre juridique actuel. Il ne semble pas opportun de reporter l'évaluation de la Commission car cela ferait courir des risques aux citoyens et serait contreproductif pour l'industrie, les incertitudes juridiques étant en effet trop nombreuses. Il serait alors plus difficile et plus coûteux de résoudre certains problèmes compliqués.

66. Parmi les mesures susceptibles d'être proposées, le CEPD recommande de prévoir un principe d'adhésion (opt-in) au point de vente. Selon ce principe, toutes les micropuces placées sur les produits de consommation seraient désactivées par défaut sur le point de vente. Il ne semble pas nécessaire ou opportun que la Commission précise la technologie spécifique à utiliser. Il serait plus approprié que la législation communautaire impose l'obligation légale d'obtenir l'adhésion des consommateurs, ce qui laisserait une certaine marge de manœuvre aux opérateurs pour décider de la façon dont ils souhaitent mettre en œuvre cette exigence.

V.4. **Autres questions à prendre en compte: la gouvernance de l'internet des objets**

67. Les informations générées par les micropuces RFID (par exemple, des informations sur les produits) pourraient à terme être interconnectées à un réseau mondial de communications. C'est ce que l'on appelle généralement l'«internet des objets». La question de la protection des données et de la vie privée est soulevée car les objets du monde réel peuvent être identifiés par les micropuces RFID, révélant alors, outre les informations sur les produits, des données à caractère personnel.

68. De nombreuses questions se posent encore quant à la responsabilité du stockage des informations générées par les micropuces. De quelle manière ce stockage sera-t-il organisé? Qui aura accès aux informations? En juin 2009, la Commission a adopté une communication sur l'internet des objets ([3]) qui identifiait clairement les problèmes potentiels de protection des données et de la vie privée liés à ce phénomène.

([1]) Communication de la Commission du 15 mars 2007 au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique», document COM(2007) 96 final.

([2]) Recommandation de la Commission du 12 mai 2009 sur la «mise en œuvre des principes de protection de la vie privée et des données personnelles dans les applications fondées sur la RFID (identification par radiofréquence)» [document C(2009) 3200 final].

([3]) Communication de la Commission du 18 juin 2009 au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «L'internet des objets: un plan d'action pour l'Europe» [document COM(2009) 278 final].

69. Le CEPD souhaite souligner certains points soulevés par la communication qui, selon lui, mériteront un examen attentif à mesure que l'internet des objets se développera. En premier lieu, une architecture décentralisée pourrait améliorer la transparence et l'applicabilité du cadre juridique communautaire. En second lieu, il est nécessaire de protéger autant que possible le droit des personnes à ne pas être suivies. En d'autres termes, le nombre de personnes suivies à l'aide d'une micropuce RFID sans l'avoir souhaité devrait être très limité. En effet, les personnes doivent adhérer explicitement. Ce dispositif est généralement appelé «droit de rester seul» ou «silence des micropuces». Enfin, dans la mise en place de l'internet des objets, la prise en compte de la vie privée dès la conception devrait être un principe directeur. Cela imposerait par exemple que des applications RFID dotées de mécanismes internes de prise de contrôle par les utilisateurs, soient dotées, dès leur conception, d'un paramétrage par défaut favorable au respect de la vie privée.

70. Le CEPD souhaiterait être consulté par la Commission au moment du déploiement des mesures envisagées dans la communication, en particulier pour la rédaction de la communication sur la vie privée et la confiance, dans une société de l'information omniprésente.

VI. **LES RÉSEAUX SOCIAUX ET L'IMPORTANCE DU PARAMÉTRAGE PAR DÉFAUT FAVORABLE AU RESPECT DE LA VIE PRIVÉE**

71. Les réseaux sociaux s'inscrivent «dans la tendance». Leur popularité semble avoir dépassé celle du courriel. Ils permettent à des personnes qui partagent certains intérêts et/ou activités de nouer des liens. Les utilisateurs peuvent afficher leur profil en ligne et partager des contenus multimédias tels que des vidéos, des photos, de la musique, ainsi que leur profil professionnel.

72. Les jeunes ont rapidement adopté la socialisation en ligne et cette tendance se confirme. En Europe, l'âge moyen des internautes a baissé au cours des dernières années: les 9-10 ans se connectent désormais plusieurs fois par semaine, et les 12-14, tous les jours, pour une durée de une à trois heures.

VI.1. **Les réseaux sociaux et le cadre juridique applicable pour la protection et la confidentialité des données**

73. Le développement des réseaux sociaux permet aux utilisateurs de poster sur internet des informations qui les concernent ou concernent des tiers. Ce faisant, selon le groupe de travail article 29 ([1]), les internautes agissent comme des «responsables du traitement des données» tel que ce terme est défini à l'article 2, point d), de la directive relative à la protection des données, en ce qui concerne les données qu'ils téléchargent vers internet ([2]). Cependant, dans la majorité des cas, ce type de traitement relève de l'exception prévue à l'article 3, paragraphe 2, de la directive: «traitement effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques». Parallèlement, les services de socialisation en ligne sont considérés comme des responsables du traitement des données puisqu'ils fournissent les moyens de traiter les données provenant des utilisateurs et l'ensemble des services de base de gestion des utilisateurs (par exemple l'enregistrement et la suppression de comptes).

74. En termes juridiques, cela signifie que les internautes et les services de socialisation en ligne partagent la responsabilité du traitement des données à caractère personnel en tant que «responsables du traitement des données», tel que ce terme est défini à l'article 2, point d), de la directive, à des degrés différents, et avec des obligations différentes.

75. Dès lors, les utilisateurs devraient réaliser et comprendre qu'en traitant leurs propres données et celles d'autres personnes, ils tombent sous le coup de la législation communautaire sur la protection des données, laquelle impose notamment d'obtenir le consentement éclairé des personnes concernées et de leur accorder un droit de rectification, de contestation, etc. De même, les services de socialisation en ligne doivent, entre autres choses, mettre en œuvre les mesures techniques et d'organisation appropriées pour prévenir tout traitement non autorisé, en tenant compte des risques présentés par le traitement et de la nature des données. Cela signifie par conséquent que les services de socialisation en ligne devraient être dotés d'un paramétrage par défaut favorable au respect de la vie privée, y compris un paramétrage restreignant l'accès au profil d'utilisateur aux contacts personnels et sélectionnés par l'utilisateur lui-même. Le paramétrage devrait aussi demander le consentement de la personne concernée avant de rendre son profil d'utilisateur accessible à des tiers, et les profils d'utilisateur à accès restreint ne devraient pas pouvoir être consultés à partir de moteurs de recherche.

76. Il existe malheureusement un écart entre les dispositions légales et la pratique actuelle. Si, d'un point de vue juridique, les internautes sont considérés comme des responsables du traitement des données et sont liés par le cadre juridique européen sur la protection des données et de la vie privée, ils ignorent en réalité bien souvent ce rôle. Ils ne comprennent en général pas très bien qu'ils traitent des données à caractère personnel et que la publication de telles informations entraîne des risques pour la protection de leur vie privée et de leurs données. Les jeunes, en particulier, publient des contenus en ligne et sous-estiment les conséquences que cela pourrait avoir pour eux-mêmes et les autres lors d'une future inscription dans un établissement scolaire ou au moment de postuler pour un emploi pour ne citer que deux exemples.

([1]) Voir l'avis n° 163, 5/2009, du groupe de travail article 29, sur la socialisation en ligne, adopté le 12 juin 2009.

([2]) «Responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire.

77. Parallèlement, les prestataires de services de socialisation en ligne présélectionnent souvent un paramétrage par défaut basé sur des options de refus (opt-out), ce qui favorise la divulgation d'informations personnelles. Certains paramètrent les profils de manière à ce qu'ils soient accessibles par défaut à partir des moteurs de recherche les plus courants. On peut alors se demander si les personnes ont effectivement consenti à la divulgation de leurs données, et si les réseaux sociaux se conforment aux dispositions de l'article 17 de la directive (précitée) qui imposent certaines mesures techniques et d'organisation appropriées pour prévenir tout traitement non autorisé.

VI.2. **Les risques générés par les réseaux sociaux et les actions suggérées pour y répondre**

78. Il résulte de ce qui précède que la protection de la vie privée et des données à caractère personnel est de plus en plus menacée. À travers les réseaux sociaux, les internautes et les personnes dont les données sont téléchargées s'exposent à des violations flagrantes de leur droit à la protection de la vie privée et des données à caractère personnel.

79. En l'occurrence, la Commission devrait déterminer des moyens de réaction, possibles et souhaitables, face à cette situation. Le présent avis ne fournit pas une réponse complète à cette question, mais avance un certain nombre de suggestions nécessitant réflexion.

Investir dans l'éducation des internautes

80. La première de ces suggestions est d'investir dans l'éducation. À cet égard, les institutions communautaires et les autorités nationales devraient investir dans l'éducation et la sensibilisation des internautes aux menaces posées par les sites de socialisation en ligne. Ainsi par exemple, la DG Société de l'information a mis en place un programme intitulé «Pour un internet plus sûr» destiné à protéger les enfants et les jeunes notamment par des activités de sensibilisation, et à leur donner les moyens de se protéger sur internet ([1]). Récemment, les institutions de l'UE ont lancé une campagne intitulée «Réfléchis avant de poster» qui sensibilise le public sur les risques encourus lors du partage d'informations avec des personnes inconnues.

81. Le CEPD encourage la Commission à poursuivre son soutien à ce type d'activité. Toutefois, les prestataires de services de socialisation en ligne devraient eux aussi jouer un rôle actif car ils ont une responsabilité juridique et sociale et doivent montrer aux internautes comment utiliser leurs services de manière sûre et favorable à la protection de la vie privée.

82. Comme nous l'avons vu précédemment, les informations postées sur les réseaux sociaux sont, par défaut, accessibles de plusieurs manières. Par exemple, elles peuvent être mises à la disposition du public général, notamment par le biais des moteurs de recherche, qui les répertorient et fournissent ensuite un lien d'accès direct. D'un autre côté, l'accès aux informations peut être limité à une liste d'«amis sélectionnés» ou être entièrement privé. Évidemment, les autorisations de profil d'utilisateur et la terminologie utilisée peuvent varier d'un site web à l'autre.

83. Néanmoins, comme nous l'avons souligné ci-dessus, rares sont les utilisateurs de réseaux sociaux qui savent comment contrôler l'accès aux informations qu'ils publient, encore moins comment modifier les paramètres par défaut. Le paramétrage relatif à la vie privée n'est en général pas modifié, soit parce que les internautes ne sont pas conscients des conséquences que cela entraîne, soit par qu'ils ne savent pas comment s'y prendre. Dans la majorité des cas, le fait de ne pas modifier les paramètres ne correspond pas à une décision éclairée de partager des informations. Dès lors, les moteurs de recherche (tiers) ne devraient pas fournir de lien direct vers le profil personnel des utilisateurs, en se fondant sur la simple supposition que ces derniers ont accepté (par défaut, en ne modifiant pas le paramétrage de sécurité) de publier leurs informations sans restriction.

84. Dans ce domaine, l'éducation permettra sans doute de faire des progrès, mais ne suffira pas à elle seule. C'est pourquoi, comme le recommande le groupe de travail article 29 dans son avis sur les réseaux sociaux, les prestataires de services de socialisation devraient proposer gratuitement un paramétrage par défaut favorable au respect de la vie privée. Cela sensibiliserait les utilisateurs et leur permettrait de faire des choix plus réfléchis quant au partage et aux destinataires de leurs informations.

Le rôle de l'auto-régulation

85. La Commission a conclu un accord avec vingt prestataires de services de socialisation en ligne intitulé «Principes de l'UE pour des réseaux sociaux plus sûrs» ([2]). L'objectif de cet accord est d'améliorer la sécurité des mineurs lorsqu'ils se rendent sur des sites de socialisation sur internet en Europe. Les principes énoncés reprennent de nombreuses exigences établies par le cadre juridique européen décrit ci-dessus. Ils comprennent, par exemple, l'obligation de donner les moyens aux utilisateurs, par des outils et des dispositifs technologiques, de contrôler l'utilisation et la diffusion de leurs informations personnelles. Ils prévoient également des paramètres par défaut favorables à la protection de la vie privée.

86. Début janvier 2010, la Commission a publié les conclusions de son rapport d'évaluation sur la mise en œuvre des principes ([3]). Le CEPD se montre préoccupé car le rapport souligne que certaines mesures ont été prises, mais que nombre d'autres sont restées lettre morte. Le

([1]) Des informations sur ce programme sont disponibles à l'adresse suivante: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Disponibles à l'adresse: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Rapport d'évaluation sur la mise en œuvre des principes de l'UE pour des réseaux sociaux plus sûrs: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

rapport pointe par exemple certains problèmes relatifs à la communication des mesures et des outils de sécurité sur les sites. Il montre aussi que moins de 50 % des signataires de l'accord restreignent l'accès au profil d'utilisateur des mineurs à leurs seuls amis.

Vers l'obligation de paramètres par défaut favorables à la protection de la vie privée

87. Dans ce contexte, la question clé est la suivante: faut-il prendre des mesures supplémentaires pour contraindre les prestataires de services de socialisation en ligne à fournir des paramètres par défaut favorables à la protection de la vie privée? Viviane Reding, l'ancienne commissaire à la société de l'information, avait évoqué l'éventualité d'un recours à une telle législation ([1]). Le Comité économique et social a par ailleurs déclaré qu'un texte devrait imposer des normes de protection minimale pour compléter l'autorégulation ([2]).

88. Comme indiqué précédemment, l'article 17 de la directive sur la protection des données impose déjà indirectement aux prestataires de services de socialisation de mettre en place des paramètres par défaut favorables à la protection de la vie privée ([3]). Il oblige les responsables du traitement des données à «prendre les mesures techniques et d'organisation appropriées (tant au moment de la conception qu'à celui de la mise en œuvre du traitement, et du traitement lui-même) en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé, [en] tenant compte des risques présentés par les traitements et de la nature des données à protéger».

89. Toutefois, l'article 17 est beaucoup trop vague et imprécis dans le contexte présent. En effet, il n'indique pas clairement ce qu'il faut entendre par mesures techniques et d'organisation appropriées dans le cadre précis des réseaux sociaux. Nous nous trouvons donc face à une incertitude juridique problématique, tant pour les organismes de réglementation que pour les particuliers, dont les données à caractère personnel et la vie privée ne sont pas bien protégées.

90. Pour ces raisons, le CEPD prie instamment la Commission d'élaborer une législation prévoyant au moins l'obligation de fournir des services dotés de paramètres par défaut favorables à la protection de la vie privée, et assortie d' exigences plus précises:

a) Fourniture de paramètres permettant de restreindre l'accès aux profils d'utilisateur aux seuls contacts sélectionnés par l'utilisateur même. Les paramètres doivent aussi exiger que l'utilisateur consente de manière affirmative à ce que son profil d'utilisateur soit accessible par des tiers.

b) Les profils d'utilisateur à accès restreint ne doivent pas pouvoir être consultés par le biais de moteurs de recherche internes/externes.

91. Outre cette obligation de paramétrage par défaut, une question reste posée: existe-t-il d'autres mesures appropriées permettant de protéger les données (dans le domaine de la protection des mineurs par exemple)? Ceci soulève la question plus large de savoir s'il serait approprié d'établir un cadre propre à ce type de services, qui, outre le paramétrage par défaut obligatoire, permettrait de réglementer d'autres aspects. Le CEPD demande à la Commission de réfléchir à ces questions.

VII. **PARAMÈTRES DU NAVIGATEUR PAR DÉFAUT FAVORABLES À LA PROTECTION DE LA VIE PRIVÉE ET PERMETTANT DE SOUSCRIRE DE MANIÈRE INFORMÉE À LA RÉCEPTION DE MESSAGES PUBLICITAIRES**

92. Les prestataires de services de publicité par internet utilisent des cookies et d'autres dispositifs pour suivre le comportement des consommateurs lorsqu'ils surfent sur internet, ce qui leur permet ensuite de dresser la liste de leurs intérêts et d'établir leur profil de consommateur. Ces informations sont alors exploitées pour cerner les internautes et leur envoyer des messages publicitaires ciblés ([4]).

VII.1. **Les défis à relever et les risques qui persistent avec le cadre juridique actuel relatif à la protection des données et de la vie privée**

93. Ce traitement est couvert par la directive sur la protection des données (lorsque des données à caractère personnel sont concernées) ainsi que par l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques». Il exige de manière claire que l'utilisateur soit informé de la possibilité que des «cookies» ou d'autres éléments soient stockés sur son disque dur, et qu'il ait la possibilité de réagir en donnant son consentement ou en refusant ledit stockage ([5]).

94. À ce jour, les prestataires de services publicitaires sur internet se sont appuyés sur les paramètres de navigateur et les politiques générales relatives à la protection de la vie

([1]) Viviane Reding, commissaire européenne chargée des questions liées à la société de l'information et du programme «Réfléchis avant de poster!». Comment rendre les réseaux internet de socialisation plus sûrs pour les enfants et les adolescents? Journée pour un internet plus sûr, Strasbourg, 9 février 2010.

([2]) Avis du Comité économique et social européen: «L'impact des réseaux de socialisation et leur interaction dans le domaine du citoyen/consommateur», 4 novembre 2009.

([3]) Également développé au point 33 du présent document.

([4]) Les «tracking cookies» sont de petits fichiers texte qui contiennent un numéro d'identification unique. En général, les prestataires de services publicitaires sur internet (ainsi que les opérateurs et les éditeurs web) placent ces cookies sur le disque dur de l'internaute, en particulier dans son navigateur, lorsqu'il visite pour la première fois un site web publicitaire qui fait partie de leur réseau. Le cookie permettra au prestataire de reconnaître un internaute qui revient sur ce site ou qui consulte un site partenaire du réseau publicitaire. Ces consultations répétées permettent ensuite au prestataire d'établir le profil de consommation de l'internaute.

([5]) L'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques» a récemment été modifié pour renforcer la protection contre l'interception des communications des internautes notamment par l'intermédiaire d'espiogiciels (spyware) et de cookies stockés sur leur ordinateur ou d'autres appareils. Selon la nouvelle directive, les utilisateurs devraient être mieux informés et se voir proposer des moyens de contrôle du stockage des cookies plus simples sur leurs terminaux informatiques.

privée pour informer les utilisateurs et leur permettre d'accepter ou de refuser les cookies. Dans les messages de protection de la vie privée des éditeurs de sites internet, ils indiquent la marche à suivre pour refuser les cookies ou les accepter au cas par cas. Ce faisant, ils s'efforcent de remplir leur obligation consistant à permettre aux utilisateurs d'exercer leur droit de refuser les cookies.

95. Si, en théorie, cette méthode (reposant sur les navigateurs) pouvait effectivement donner lieu à un consentement éclairé des internautes, la réalité est tout autre. En effet, les internautes n'ont en général qu'une compréhension partielle de la problématique de la collecte d'informations (surtout par des tiers), de la valeur de ces données, de leur utilisation, du procédé technologique utilisé, et plus particulièrement, de la manière et des outils permettant de refuser les cookies. Les modalités de refus (opt-out) leur semblent non seulement compliquées, mais aussi excessives (l'utilisateur doit régler son navigateur pour accepter les cookies, puis exercer son droit de refus).

96. De ce fait, peu de personnes exercent leur droit de refus des cookies, non pas en vertu d'une décision éclairée d'accepter des publicités comportementales, mais plutôt parce qu'ils ne réalisent pas qu'en n'utilisant pas leur droit de refus, ils acceptent les cookies de fait.

97. Par conséquent, si, du strict point de vue juridique, l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques» constitue une protection efficace, en pratique, les internautes sont réputés accepter d'être surveillés à des fins publicitaires et, dans de nombreux cas, voire dans la majorité des situations, ils ne sont pas du tout conscients de l'existence de cette surveillance.

98. Le groupe de travail article 29 prépare actuellement un avis destiné à clarifier les exigences légales relatives aux activités de publicité comportementale, ce qui constitue une initiative bienvenue. Néanmoins, il se pourrait que son interprétation ne suffise pas à elle seule à résoudre la problématique, et l'Union européenne pourrait bien devoir légiférer à nouveau.

VII.2. **Nécessité d'une action supplémentaire prévoyant notamment l'obligation d'un paramétrage par défaut favorable à la protection de la vie privée**

99. Comme indiqué précédemment, les navigateurs permettent en général d'exercer un certain degré de contrôle sur différents types de cookies. Actuellement, les paramètres par défaut de la majorité des navigateurs acceptent tous les cookies. En d'autres termes, les navigateurs sont systématiquement paramétrés pour accepter tous les cookies, quels qu'en soient les objectifs. Comme nous l'avons déjà indiqué, pour ne pas recevoir de cookies, l'utilisateur doit modifier les paramètres de son navigateur, ce que peu d'internautes font. En outre, aucun assistant (wizard) de protection de la vie privée n'est disponible lors de l'installation initiale ou de la première mise à jour des applications de navigateur.

100. Pour maîtriser ce problème, il faudrait que les navigateurs soient fournis avec un paramétrage par défaut favorable à la protection de la vie privée. En d'autres termes, il faudrait qu'ils soient fournis avec un réglage «refus des cookies de tiers». Pour compléter ce dispositif et le rendre plus efficace, les navigateurs devraient imposer aux utilisateurs de suivre un assistant de protection de la vie privée lorsqu'ils installent ou mettent à jour leur navigateur pour la première fois. Les utilisateurs devraient aussi bénéficier d'une plus grande granularité (mode d'effaçage par blocs d'octets) et d'informations claires sur les différents types de cookies et l'utilité de certains d'entre eux. Les internautes qui sont prêts à être surveillés afin de recevoir des publicités seront dûment informés, et devront modifier le paramétrage de leur navigateur. Cela leur permettra de mieux contrôler leurs données à caractère personnel, ainsi que leur vie privée. Cela constituerait aux yeux du CEPD, un moyen efficace de respecter et de protéger les données d'utilisateur ([1]).

101. Compte tenu, d'une part, de l'étendue du problème, c'est-à-dire du nombre d'internautes actuellement surveillés sur la base d'un consentement illusoire et, d'autre part, de la taille des intérêts en jeu, la nécessité de mettre en place des moyens supplémentaires de protection se fait de plus en plus pressante. La mise en œuvre du principe de respect de la vie privée dès la conception dans les applications de navigateur pourrait constituer une avancée majeure en direction d'un meilleur contrôle par les citoyens des pratiques de collecte de données à des fins publicitaires.

102. Pour ces raisons, le CEPD appelle la Commission à envisager des mesures législatives imposant l'intégration de paramètres par défaut favorables au respect de la vie privée dans les navigateurs, ainsi que la communication des informations pertinentes.

VIII. **AUTRES PRINCIPES VISANT À PROTÉGER LA VIE PRIVÉE ET LES DONNÉES DES PERSONNES**

103. Si le principe de respect de la vie privée dès la conception présente un potentiel important d'amélioration de la protection des données et de la vie privée, des textes juridiques complémentaires de mise en œuvre de ce principe seront nécessaires pour obtenir la confiance des consommateurs à l'égard des TIC. Dans ce contexte, le CEPD évoque le principe de transparence et l'élaboration d'un cadre obligatoire multisectoriel concernant les failles de sécurité.

VIII.1. **Le principe de responsabilité pour garantir la conformité avec le principe de respect de la vie privée dès la conception**

104. Le document publié par le groupe de travail Article 29 intitulé «L'avenir de la vie privée» ([2]) recommandait d'inclure le principe de responsabilité dans la directive

([1]) Parallèlement, le CEPD est conscient du fait que ce dispositif ne résoudrait pas entièrement le problème car certains cookies ne peuvent pas être maîtrisés par l'intermédiaire d'un navigateur, comme c'est par exemple le cas des cookies dénommés «flash cookies». Il faudrait pour cela que les développeurs de navigateurs intègrent des contrôles flash par défaut dans leurs dispositifs de contrôle des cookies sur les nouveaux navigateurs.

([2]) Voir l'Avis n° 168 du groupe de travail article 29 sur l'avenir de la protection de la vie privée — Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009.

sur la protection des données. Ce dernier, qui est déjà reconnu par certains instruments juridiques internationaux relatifs à la protection des données ([1]), exige des organisations qu'elles mettent en œuvre des processus permettant de se conformer aux lois existantes ainsi que des méthodes d'évaluation et de démonstration de cette conformité avec la législation/d'autres instruments juridiques contraignants.

105. Le CEPD soutient entièrement cette recommandation du groupe de travail article 29. Il considère que ce principe sera très pertinent pour favoriser l'application effective des principes et obligations en matière de protection des données. L'exigence de responsabilité imposera aux responsables du traitement des données de prouver qu'ils ont mis en place les mécanismes nécessaires pour se conformer à la législation sur la protection des données. Une telle approche est susceptible de participer à l'intégration concrète du principe de respect de la vie privée dès la conception dans les technologies TIC en tant qu'élément particulièrement adapté à faire toute la transparence.

106. Pour mesurer et prouver leur responsabilité, les responsables du traitement des données pourraient recourir à des procédures internes et aux services de tiers, ou à d'autres types de vérification, qui leur attribueraient éventuellement un agrément. Dans ce contexte, le CEPD prie instamment la Commission de déterminer si, outre un principe général, il convient d'imposer par la loi des mesures spécifiques de transparence, telles que, par exemple, l'obligation de procéder à des évaluations d'impact sur la protection de la vie privée et des données et, le cas échéant, dans quelles circonstances.

VIII.2. **Failles de sécurité: compléter le cadre juridique**

107. Les amendements apportés l'année dernière à la directive «Vie privée et communications électroniques» obligent à notifier les failles de sécurité aux personnes affectées, ainsi qu'aux autorités compétentes. De manière générale, une faille de sécurité se définit comme toute faille conduisant à la destruction, la perte, la divulgation, etc. de données à caractère personnel transmises, stockées ou autrement traitées, en rapport avec le service. Les personnes concernées devront être averties si la faille de sécurité est susceptible d'avoir un effet négatif sur les données à caractère personnel qui les concernent ou sur leur vie privée. Cela pourrait être le cas si la faille donnait lieu à une usurpation d'identité, une humiliation importante ou un préjudice de réputation. Les autorités compétentes devront également être prévenues de toute faille de sécurité, que celle-ci représente ou non un risque pour les personnes.

L'application des obligations relatives aux failles de sécurité dans différents secteurs

108. Malheureusement, cette obligation ne concerne que les services de communications électroniques proposés au public par les sociétés de téléphonie, les fournisseurs d'accès internet, les fournisseurs de messagerie électronique, etc. Le CEPD prie instamment la Commission de faire des propositions multisectorielles sur les failles de sécurité. En termes de contenu, le CEPD considère que le cadre juridique relatif aux failles de sécurité intégré dans la directive «Vie privée» établit un juste équilibre entre la protection des droits des personnes (y compris leur droit à la protection des données à caractère personnel et de leur vie privée) et les obligations imposées aux entités concernées. Parallèlement, il s'agit d'un cadre bien réel et «mordant», car il s'appuie sur des dispositions d'application importantes et attribue aux autorités les prérogatives nécessaires pour enquêter et prendre des sanctions en cas de non-respect.

109. Par conséquent, le CEPD prie instamment la Commission d'adopter une proposition législative qui permettrait d'appliquer ce cadre dans plusieurs secteurs, après ajustement si nécessaire. Cela garantirait aussi l'harmonie des normes et des procédures appliquées dans les différents secteurs.

Compléter le cadre juridique intégré dans la directive «Vie privée et communications électroniques» par la comitologie

110. La directive «Vie privée et communications électroniques» permet à la Commission d'adopter des mesures de mise en œuvre technique, à savoir des mesures précises concernant la notification des failles de sécurité, par le biais d'une procédure de comitologie ([2]). Cette délégation de responsabilités est destinée à garantir la mise en œuvre et l'application cohérentes du cadre juridique relatif aux failles de sécurité. Une mise en œuvre cohérente permettrait aussi de garantir le même niveau de protection élevé à tous les citoyens européens, et d'éviter d'accabler les entités concernées avec des exigences multiples et divergentes en matière de notification.

111. La directive «Vie privée et communications électroniques» a été adoptée en novembre 2009. Rien ne semble justifier un report du début des travaux pour l'adoption des mesures de mise en œuvre technique. Le CEPD a organisé deux séminaires destinés à rassembler et partager des expériences sur la notification des failles de sécurité. Il serait heureux de partager les résultats de cet exercice et attend avec intérêt de travailler prochainement avec la Commission et d'autres parties prenantes pour affiner le cadre juridique global sur les failles de sécurité.

112. Le CEPD prie instamment la Commission de prendre les mesures nécessaires, et ce dans les meilleurs délais. Avant d'adopter des mesures de mise en œuvre technique, la Commission devra engager une large consultation à laquelle participeront l'ENISA, le CEPD et le groupe de travail article 29. La consultation englobera aussi d'autres «parties prenantes concernées» afin, notamment, de tenir compte des moyens techniques et économiques les plus appropriés pour la mise en œuvre.

([1]) «Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel» de l'OCDE (1980). Déclaration de Madrid du 3 novembre 2009: «Standards mondiaux de respect de la vie privée dans un monde globalisé».

([2]) La comitologie correspond à l'adoption de mesures de mise en œuvre technique par l'intermédiaire d'un comité composé de représentants des États membres et présidé par la Commission. Selon la directive «Vie privée et communications électroniques», cette procédure dite «de réglementation avec contrôle» s'applique, ce qui signifie que le Parlement européen et le Conseil peuvent s'opposer aux mesures proposées par la Commission. Plus d'informations: http://europa.eu/scadplus/glossary/comitology_fr.htm

IX. **CONCLUSIONS**

113. La confiance — ou plutôt l'absence de confiance — a été identifiée comme un élément clé dans l'émergence et le déploiement réussi des technologies de l'information et de la communication. Si les personnes ne font pas confiance aux TIC, ces technologies finiront par disparaître. La confiance dans les TIC dépend de différents facteurs. S'assurer que ces technologies n'empiètent pas sur les droits fondamentaux des individus à la protection de leur vie privée et de leurs données personnelles, en est un.

114. Pour renforcer encore le cadre juridique sur la protection des données/de la vie privée, dont les principes restent entièrement valables dans la société de l'information, le CEPD propose à la Commission d'intégrer le principe de respect de la vie privée dès la conception à différents niveaux du droit et du processus politique.

115. Il recommande à la Commission de suivre les quatre étapes suivantes:

a) Proposer d'intégrer une disposition générale sur le respect de la vie privée dès la conception dans les textes juridiques relatifs à la protection des données. Cette disposition devrait être neutre sur le plan technologique, et la conformité devrait être obligatoire à différents niveaux.

b) Formuler cette disposition générale sous forme de dispositions spécifiques lorsque différents instruments juridiques seront proposés, dans différents secteurs. Ces dispositions spécifiques pourraient déjà être intégrées dans l'appareil juridique, sur la base de l'article 17 de la directive sur la protection des données à caractère personnel (et d'autres textes législatifs).

c) Intégrer le principe de respect de la vie privé dès la conception dans le programme numérique européen, en tant que principe directeur.

d) Introduire le principe dans d'autres initiatives communautaires (principalement des initiatives non législatives).

116. Dans trois domaines TIC spécifiques, le CEPD recommande à la Commission d'évaluer la nécessité de formuler des propositions pour la mise en œuvre du principe de différentes manières:

a) Concernant la RFID, il convient de proposer des mesures législatives pour réglementer les principaux problèmes liés à l'utilisation de la RFID en cas d'échec de la mise en œuvre du cadre juridique par l'auto-régulation. Prévoir un principe d'adhésion (opt-in) sur le point de vente. En vertu de ce principe, toutes les micropuces RFID placées sur les produits de consommation seront désactivées par défaut sur le point de vente.

b) Concernant les réseaux sociaux, élaborer une législation prévoyant, à tout le moins, l'obligation généralisée de fournir des services dotés de paramètres par défaut favorables à la protection de la vie privée et des exigences plus précises restreignant l'accès au profil d'utilisateur aux seuls contacts sélectionnés par l'utilisateur, et l'impossibilité de découvrir ce profil par le biais de moteurs de recherche internes/externes.

c) Concernant les messages publicitaires ciblés, la législation pourrait imposer un refus des cookies de tiers intégré par défaut dans le paramétrage des navigateurs et imposer aux internautes de suivre les étapes d'un «assistant de confidentialité» lors de la première installation du navigateur ou de sa mise à jour.

117. Enfin, le CEPD suggère à la Commission:

a) de réfléchir à une éventuelle mise en œuvre du principe de responsabilité dans la directive sur la protection des données, et

b) de développer un ensemble de règles et de procédures visant la mise en œuvre des dispositions relatives à la notification des failles de sécurité prévues par la directive «Vie privée et communications électroniques», et en étendre généralement l'application à tous les responsables du traitement des données.

Fait à Bruxelles, le 18 mars 2010.

Peter HUSTINX

Contrôleur européen de la protection des données