Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 12695
29 juillet 2011

La protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne

Rapport[1]
Commission de la culture, de la science et de l'éducation
Rapporteure: Mme Andreja RIHTER, Slovénie, Groupe socialiste

Résumé

La numérisation des informations a engendré des possibilités jusqu'alors impensables d'identifier les individus grâce à leurs données. Celles-ci sont traitées par un nombre toujours croissant d'instances publiques et privées dans le monde. Les informations à caractère personnel sont introduites dans le cyberespace par les utilisateurs eux-mêmes et des tiers. Les individus laissent des traces de leur identité en utilisant les technologies de l'information et de la communication (TIC). L'établissement des profils d'utilisateurs de l'internet est devenu un phénomène répandu.

Le droit fondamental de chacun au respect de sa vie privée et familiale, de son domicile et de sa correspondance, tel qu'il est garanti par l'article 8 de la Convention européenne des droits de l'homme, comprend le droit à la protection des données à caractère personnel ainsi que l'obligation, à cet égard, de prévoir des garanties appropriées dans le cadre de la loi interne. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («Convention no 108») exige que ces données soient traitées loyalement et de manière sécurisée, pour des finalités déterminées et légitimes, et établit le droit de chacun de connaître, de consulter et de rectifier les données à caractère personnel traitées par des tiers ou de supprimer les données à caractère personnel qui ont été traitées sans autorisation.

Un plan d'action doit être élaboré pour la promotion des normes juridiques communes garantissant la protection de la vie privée et des données à caractère personnel dans les réseaux et services fondés sur les TIC en Europe et en dehors de celle-ci, dans le cadre de la Convention no 108.

1. Renvoi en commission: Doc. 12021, Renvoi 3608 du 2 octobre 2009.

Sommaire **Page**

A. Projet de résolution[2]

1. Tout en saluant les progrès historiques des technologies de l'information et de la communication (ci-après «TIC») et les effets positifs qui en découlent pour les individus, les sociétés et notre civilisation toute entière, l'Assemblée parlementaire note avec préoccupation que la numérisation des informations a engendré des possibilités jusqu'alors impensables d'identifier les individus grâce à leurs données. Celles-ci sont traitées par un nombre toujours croissant d'instances publiques et privées dans le monde. Les informations à caractère personnel sont introduites dans le cyberespace par les utilisateurs eux-mêmes et des tiers. Les individus laissent des traces de leur identité en utilisant les TIC. L'établissement des profils d'utilisateurs de l'internet est devenu un phénomène répandu. Les sociétés contrôlent parfois les employés et les contacts commerciaux au moyen des TIC.

2. En outre, les systèmes fondés sur les TIC sont souvent infiltrés dans le but d'obtenir des données relatives à des entités juridiques, en particulier les sociétés commerciales, les institutions financières, les institutions de recherche et les pouvoirs publics. Ce type d'accès pourrait causer des préjudices économiques au secteur privé et avoir une incidence négative sur le bien-être économique des Etats, la sûreté publique ou la sécurité nationale.

3. L'Assemblée s'alarme de cette évolution qui remet en cause le droit à la vie privée et à la protection des données. Dans un Etat démocratique régi par la prééminence du droit, le cyberespace ne doit pas être considéré du point de vue juridique comme un espace de non-droit.

4. L'Assemblée rappelle le droit fondamental de chacun au respect de sa vie privée et familiale, de son domicile et de sa correspondance tel qu'il est garanti par l'article 8 de la Convention européenne des droits de l'homme (STE n° 5). Ce droit comprend le droit à la protection des données à caractère personnel ainsi que l'obligation, à cet égard, de prévoir des garanties appropriées dans le cadre de la loi interne.

5. L'Assemblée souligne la nécessité d'éradiquer l'utilisation des TIC pour posséder ou transmettre du matériel pornographique impliquant des enfants, en accord avec la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

6. Rappelant qu'elle soutient de longue date la protection de la vie privée depuis sa Recommandation 509 (1968) relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes, l'Assemblée accueille avec satisfaction et appuie la Résolution n° 3 sur la protection des données et la vie privée au troisième millénaire, qui a été adoptée lors de la 30e Conférence des Ministres de la Justice du Conseil de l'Europe (Istanbul, 24-26 novembre 2010).

7. Comme l'Assemblée le déclarait dans sa Résolution 428 (1970) sur les moyens de communication de masse et les droits de l'homme, «lorsque des banques régionales, nationales ou internationales de données informatiques sont instituées, l'individu ne doit pas être rendu totalement vulnérable par l'accumulation d'informations concernant sa vie privée. Ces centres doivent enregistrer uniquement le minimum de renseignements nécessaires.»

8. Faisant référence à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après «Convention n° 108»), l'Assemblée souligne que le droit à la protection des données à caractère personnel comprend notamment le droit à ce que ces données soient traitées loyalement et de manière sécurisée, pour des finalités déterminées et légitimes, et le droit de chacun de connaître, de consulter et de rectifier les données à caractère personnel traitées par des tiers ou de supprimer les données à caractère personnel qui ont été traitées sans autorisation. Le respect de ces obligations doit être supervisé par une autorité indépendante conformément au Protocole additionnel à la Convention n° 108, concernant les autorités de contrôle et les flux transfrontières de données (STCE n° 181).

9. L'Assemblée réaffirme que les Etats membres ne devraient transférer des données à caractère personnel vers un autre Etat ou une organisation que si cet Etat ou cette organisation est Partie à la Convention n° 108 et à son Protocole additionnel ou assure un niveau de protection adéquat pour le transfert considéré. Les transferts de données à caractère personnel qui violent le droit à la protection de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme peuvent faire l'objet de recours devant la Cour européenne des droits de l'homme.

10. L'Assemblée se félicite que la Convention n° 108 ait été signée et ratifiée par presque tous les Etats membres du Conseil de l'Europe – à l'exception, regrettable, de l'Arménie, de la Fédération de Russie, de Saint-Marin et de la Turquie – et note que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union

2. Projet de résolution adopté à l'unanimité par la commission le 12 mai 2011.

européenne contiennent dans une large mesure les mêmes principes. Face à la mondialisation croissante des services fournis par les TIC, il est de la plus grande urgence pour toute l'Europe d'adhérer aux mêmes normes et de s'efforcer d'impliquer d'autres pays dans le monde.

11. Si l'article 17 du Pacte international relatif aux droits civils et politiques (ci-après «PIDCP») reconnaît le droit à la vie privée, l'interprétation juridique et l'application pratique de cet article restent nettement en deçà des normes européennes. L'Assemblée estime donc que toute initiative de portée mondiale devrait être fondée sur la Convention n° 108 et son Protocole additionnel, tous deux étant en principe ouverts à la signature d'Etats non membres du Conseil de l'Europe.

12. Bien que l'usage de technologies et de logiciels de prévention, la pratique de l'autorégulation volontaire par les fournisseurs de TIC et les utilisateurs privés ainsi qu'une meilleure sensibilisation des utilisateurs peuvent réduire le risque d'ingérence dans la vie privée et le traitement préjudiciable des données à caractère personnel au moyen des TIC, l'Assemblée estime que seule une législation spécifique et une mise en application effective peuvent protéger suffisamment le droit à la protection de la vie privée et des données à caractère personnel visé par l'article 17 du PIDCP et l'article 8 de la Convention européenne des droits de l'homme.

13. L'Assemblée déplore que l'absence de normes juridiques mondialement acceptées sur la protection des données concernant les réseaux et services fondés sur les TIC débouche sur une insécurité juridique et contraint les tribunaux nationaux à combler ce vide, au cas par cas, en interprétant les lois internes à la lumière de l'article 17 du PIDCP et de l'article 8 de la Convention européenne des droits de l'homme. Non seulement cela expose les individus à une protection différenciée de leurs droits, mais entraîne des exigences différentes et variables pour les fournisseurs de TIC et les utilisateurs au niveau global, ce qui rend le niveau de responsabilité pratiquement imprévisible.

14. L'Assemblée se félicite de la coopération internationale établie entre les autorités indépendantes de protection des données et appuie les efforts qu'elles déploient pour garantir une protection internationale commune de la vie privée et des données à caractère personnel face aux développements rapides des technologies, comme indiqué dans leurs résolutions adoptées à Madrid en 2009 et à Jérusalem en 2010. L'Assemblée partage leur avis selon lequel la Convention n° 108 devrait être soutenue au niveau mondial car il s'agit de l'ensemble de normes les plus avancées dans ce domaine en droit international public.

15. Rappelant la Convention sur la cybercriminalité (STE n° 185), l'Assemblée se félicite que plus de 100 Etats aient adopté une législation qui s'inspire de l'esprit de cette convention. En vertu des articles 2, 3 et 4 de ladite convention, ses parties sont tenues d'ériger en infraction pénale dans leur droit interne tout accès, interception et manipulation de données informatiques effectués sciemment sans autorisation. Ces données informatiques peuvent contenir des données à caractère personnel de personnes physiques et des données à caractère confidentiel de personnes morales qui sont présentes sur les réseaux informatiques.

16. Rappelant l'article 10 de la Convention sur les droits de l'homme et la biomédecine (STE n° 164) et l'article 16 du Protocole additionnel à cette Convention relatif aux tests génétiques à des fins médicales (SCTE n° 203), l'Assemblée insiste sur le droit de chacun à la protection des informations relatives à sa santé, notamment le droit d'être informé de toute collecte et traitement de ces données au moyen des TIC et d'y consentir ou non. Les données à caractère sanitaire et médical des personnes exigent le niveau de protection des données le plus élevé, car elles constituent l'un des éléments essentiels de la vie privée et de la dignité humaine.

17. L'Assemblée rappelle également l'obligation de respecter le droit à la vie privée et à la protection des données en vertu de la Convention sur l'accès aux documents publics (STCE n° 205) ainsi que les limites fixées à la protection des données à caractère personnel par la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n ° 198) et par la Convention concernant l'assistance administrative mutuelle en matière fiscale (STE n° 127) et son Protocole d'amendement (STCE n° 208).

18. L'Assemblée approuve les principes généraux suivants concernant la protection de la vie privée et des données à caractère personnel dans un environnement de TIC:

18.1. la protection de la vie privée est un élément nécessaire de la vie humaine et du fonctionnement humain d'une société démocratique; toute violation de la vie privée d'une personne met en jeu sa dignité, sa liberté et sa sécurité;

18.2. le droit à la protection de la vie privée et des données à caractère personnel est un droit fondamental qui impose aux Etats l'obligation de fournir un cadre juridique adéquat à une telle protection contre toute ingérence des pouvoirs publics, de simples particuliers et d'entités privées;

18.3. toute personne doit pouvoir contrôler l'utilisation que d'autres font de ses données à caractère personnel, notamment l'accès, la collecte, le stockage, la divulgation, la manipulation, l'exploitation ou autre traitement de ces données, à l'exception de la rétention licite ou techniquement nécessaire des données de trafic liées aux TIC et des données de localisation; le contrôle de l'utilisation des données à caractère personnel doit comprendre le droit de chacun de connaître et de rectifier les données qui le concernent, et de faire supprimer des systèmes et réseaux fondés sur les TIC toutes les données qui ont été fournies sans obligation juridique;

18.4. les données à caractère personnel ne doivent pas être utilisées par d'autres sans consentement préalable, ce qui exige l'expression d'un consentement en connaissance de cause concernant cette utilisation, à savoir une manifestation de volonté libre, spécifique et informée, et exclut un usage tacite ou automatique; le consentement peut être retiré par la suite à tout moment; dans ce cas, les données à caractère personnel ne peuvent plus être utilisées;

18.5. lorsque des données à caractère personnel doivent être utilisées à des fins d'exploitation commerciale, la personne concernée doit être également informée à l'avance de cette exploitation commerciale; lorsque des données à caractère personnel peuvent être utilisées par d'autres, parce que la personne concernée a donné son accord ou parce que ces données, par ailleurs anonymes, sont accessibles au public, l'accumulation, l'interconnexion, la personnalisation et l'utilisation intentionnelles de ces données accumulées exigent toutefois le consentement de la personne concernée;

18.6. les systèmes TIC personnels ainsi que les communications fondés sur des TIC ne doivent pas être infiltrés ou manipulés si une telle action viole la vie privée ou le secret de la correspondance; l'accès et la manipulation sans autorisation au moyen de «cookies» ou d'autres dispositifs automatisés non autorisés constituent une violation de la vie privée, en particulier lorsque cet accès ou cette manipulation servent d'autres intérêts, notamment commerciaux;

18.7. un degré de protection supérieur doit être accordé aux images privées, aux données à caractère personnel des mineurs ou des personnes souffrant d'un handicap mental ou psychologique, aux données personnelles ethniques, aux données personnelles sanitaires, médicales ou sexuelles, aux données personnelles biométriques et génétiques, aux données personnelles politiques, philosophiques ou religieuses, aux données financières à caractère personnel et à d'autres informations qui relèvent du domaine essentiel de la vie privée; un degré de protection supérieur doit être également accordé aux données à caractère personnel liées aux poursuites judiciaires ou au secret professionnel des juristes, des professionnels de la santé et des journalistes; ce degré de protection supérieur peut être assuré par des moyens d'autorégulation, des moyens techniques et des moyens juridiques qui permettent de rendre dûment responsables ceux qui violent la protection des données ou la vie privée; il conviendrait de fixer des délais au-delà desquels de telles données ne pourraient plus être conservées ou utilisées;

18.8. les entités publiques et privées qui collectent, stockent, traitent ou utilisent des données à caractère personnel doivent être tenues de réduire le volume de ces données au plus strict minimum nécessaire; les données à caractère personnel doivent être supprimées lorsqu'elles sont obsolètes ou inutilisées ou lorsque la finalité de leur collecte a été atteinte ou n'existe plus; la collecte et le stockage aléatoires de données à caractère personnel doivent être évités;

18.9. toute personne doit pouvoir disposer d'un recours efficace devant les tribunaux nationaux contre toute ingérence illicite dans son droit à la protection de sa vie privée et de ses données à caractère personnel; des organes d'autorégulation et d'arbitrage volontaire ainsi que des autorités indépendantes de protection des données doivent compléter le système judiciaire afin de garantir la protection efficace de ce droit; les pouvoirs publics et les sociétés commerciales doivent être encouragés à élaborer des mécanismes permettant de recevoir et de traiter les plaintes émanant d'individus qui allèguent que leur droit à la protection de leurs données ou de leur vie privée a été violé, ainsi que des mécanismes garantissant le respect au niveau interne du droit à la protection de la vie privée et des données à caractère personnel; toute violation de la protection de la vie privée et des données à caractère personnel doit être sanctionnée pénalement.

19. L'Assemblée se félicite que les Parties à la Convention n° 108 aient commencé à préparer une révision possible de cette convention suite à l'évolution rapide des technologies et à la concurrence commerciale de plus en plus agressive qui règne dans les services fondés sur les TIC.

20. C'est pourquoi l'Assemblée invite:

20.1. les parlements d'Arménie, de la Fédération de Russie, de Saint-Marin et de Turquie à lancer sans délai leur processus de ratification de la Convention n° 108, ce qui permettra à leurs pays de jouer un rôle actif dans l'évolution ultérieure de cette convention;

20.2. ses délégations d'observateurs du Canada, d'Israël et du Mexique à lancer un débat dans leurs parlements respectifs sur la signature et la ratification de la Convention n° 108 et la participation à son évolution ultérieure. Les délégations d'observateurs sont invitées à faire rapport sur les progrès accomplis à cet égard à l'Assemblée en temps utile;

20.3. les autres Etats qui coopèrent avec le Conseil de l'Europe, en particulier les Etats observateurs du Conseil de l'Europe que sont le Japon, les Etats-Unis d'Amérique et le Saint-Siège, à encourager leurs autorités à adhérer à la Convention n° 108;

20.4. la Commission européenne pour la démocratie par le droit (Commission de Venise) à faire rapport à l'Assemblée sur le degré de conformité de la législation interne de ses Etats membres et observateurs avec le droit fondamental et universel à la protection de la vie privée et des données à caractère personnel à la lumière de la Convention n° 108 et de son Protocole additionnel, et sur l'intention éventuelle des Etats qui ne sont pas encore parties à cette convention de la signer et de la ratifier.

21. L'Assemblée demande au Secrétaire Général du Conseil de l'Europe:

21.1. de rechercher un appui à haut niveau des Nations Unies pour inciter les Etats à adhérer à la Convention n° 108, par le biais notamment du Forum des Nations Unies sur la gouvernance de l'internet, de l'Union internationale des télécommunications et de Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO);

21.2. d'adopter des règles et réglementations internes particulières pour garantir la protection de la vie privée et des données à caractère personnel du personnel du Conseil de l'Europe ainsi que des membres des organes du Conseil. L'utilisation généralisée des TIC au sein du Conseil de l'Europe et son statut juridique extraterritorial ne doivent pas nuire à la protection de la vie privée et des données à caractère personnel. Dans ce contexte, la position et les activités du Commissaire à la protection des données du Conseil de l'Europe devraient être renforcées et le cadre réglementaire interne révisé en conséquence.

22. L'Assemblée appelle l'Union européenne à soutenir une large adhésion à la Convention n° 108 et à son Protocole additionnel, et à en devenir elle-même partie quand les amendements nécessaires pour permettre cette adhésion seront entrés en vigueur.

23. Se félicitant des efforts déployés au niveau international par les différentes parties prenantes pour garantir le droit à la protection des données à caractère personnel dans un environnement fondé sur les TIC, tels que les résolutions de Madrid (2009) et de Jérusalem (2010) adoptées par des autorités indépendantes de protection des données, ainsi que des diverses initiatives conduites par la Chambre internationale de commerce dans le domaine de la protection des données, l'Assemblée invite toutes les parties prenantes à joindre leurs forces à celles du Conseil de l'Europe afin que les initiatives individuelles n'entrent pas en contradiction les unes avec les autres ou risquent d'être utilisées pour brouiller une approche commune du droit universel au respect de la vie privée et des données à caractère personnel ou pour affaiblir les normes juridiques existantes.

B. Projet de recommandation[3]

1. Faisant référence à sa Résolution ... (2011) sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne, l'Assemblée parlementaire accueille avec satisfaction et appuie la Résolution n° 3 sur la protection des données et la vie privée au troisième millénaire adoptée lors de la 30e Conférence des Ministres de la justice du Conseil de l'Europe (Istanbul, 24-26 novembre 2010) et demande un plan d'action pour la promotion de normes juridiques communes garantissant la protection de la vie privée et des données à caractère personnel dans les réseaux et services fondés sur les technologies de l'information et de la communication (TIC) en Europe et en dehors de celle-ci, dans le cadre de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après «Convention n° 108»).

2. L'Assemblée recommande que le Comité des Ministres:

2.1. recherche activement la signature et la ratification de la Convention n° 108 et de son Protocole additionnel (STE n° 181) par l'Union européenne et les Etats membres qui ne l'ont pas fait à ce jour, et demande aux Parties à la Convention n° 108, qui ne l'ont pas encore fait, d'accepter les amendements permettant l'adhésion de l'Union européenne à cette convention;

2.2. encourage et soutient, en s'appuyant sur les Représentations permanentes des Etats membres du Conseil de l'Europe auprès des Nations Unies, la signature et la ratification de la Convention n° 108 par les Etats non-membres, en particulier les Etats qui sont observateurs auprès du Conseil de l'Europe ou sont parties à des accords partiels élargis ou ont signé d'autres conventions du Conseil de l'Europe;

2.3. prévoie un budget adéquat au sein du secrétariat du Conseil de l'Europe pour faire évoluer juridiquement la Convention n° 108 suivant la Résolution n° 3 de la 30e Conférence des Ministres de la Justice du Conseil de l'Europe, et demande aux Etats membres et observateurs ainsi qu'à l'Union européenne de fournir à titre volontaire des fonds supplémentaires pour ces activités;

2.4. invite les Parties à la Convention n° 108:

2.4.1. à prendre en compte la Résolution …. (2011) de l'Assemblée lors de la révision de la convention;

2.4.2. à ne pas réduire le niveau de protection existant de la vie privée et des données à caractère personnel;

2.4.3. à établir un mécanisme de suivi de la conformité des Parties aux obligations qu'elles ont contractées en vertu de cette convention;

2.4.4. à tenir compte de la Résolution 1744 (2010) de l'Assemblée sur les acteurs extra-institutionnels dans le système démocratique lorsqu'elles consultent des parties prenantes privées;

2.5. encourage tous les Etats membres et les Etats non-membres à signer et à ratifier la Convention sur la cybercriminalité (STE n° 185);

2.6. encourage tous les Etats membres et les Etats non-membres à signer et à ratifier la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (SCTE n° 201);

2.7. demande à ses instances compétentes en matière de bioéthique de proposer des normes relatives au traitement par les TIC des données sanitaires et médicales dans le cadre de la Convention sur les droits de l'homme et la biomédecine (STE n° 164) et ses protocoles additionnels;

2.8. porter cette Recommandation et la Résolution …. (2011) à l'attention des ministères compétents et des autorités chargées de la protection des données dans les Etats membres.

3. Projet de recommandation adopté à l'unanimité par la commission le 12 mai 2011.

C. Exposé des motifs, par Mme Rihter, rapporteur

1. Introduction

1.1. Préparation du rapport

1. Après avoir soumis une proposition relative au respect de la vie privée et la gestion des informations à caractère personnel sur l'internet et d'autres médias en ligne[4], j'ai été nommée rapporteur par la commission de la culture, de la science et de l'éducation le 8 décembre 2009. Ayant exercé les fonctions de ministre de la Culture de la Slovénie de 2000 à 2004, les politiques relatives aux médias ainsi que les nouveaux médias sont des thèmes auxquels je suis sensible.

2. La sous-commission des médias a organisé le Forum ouvert du Conseil de l'Europe sur la vie privée et la liberté de l'internet dans le cadre du Forum des Nations Unies sur la gouvernance de l'internet, qui s'est tenu à Vilnius (Lituanie) le 15 septembre 2010. Ce forum ouvert a permis aux experts invités et aux parties prenantes au Forum sur la gouvernance de l'internet d'exprimer leurs avis sur ce thème au début de la préparation du présent rapport[5].

3. Je tiens à saluer en particulier les contributions de Mme Maud de Boer-Buquicchio, Secrétaire Générale adjointe du Conseil de l'Europe, de Mme Catherine Pozzo di Borgo, vice-présidente du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE no 108, ci-après «Convention no 108») et commissaire adjointe du gouvernement auprès de la Commission nationale de l'informatique et des libertés (CNIL, Paris), de M. Richard Allan, directeur des Questions réglementaires européennes pour Facebook (Londres), de Mme Katitza Rodríguez, directrice, chargée des questions liées aux droits internationaux à l'Electronic Frontier Foundation et membre du conseil consultatif de Privacy International (San Francisco), et de M. Peng Hwa Ang, professeur à l'université technologique de Nanyang à Singapour.

4. Mme Cécile de Terwangne et M. Jean-Noël Colin, professeurs à l'université de Namur (Belgique), ont été invités à préparer, selon les axes thématiques convenus avec moi-même, un rapport général sur les défis techniques et juridiques posés à la vie privée et à la protection des données dans le cyberespace d'aujourd'hui. Ils ont présenté leur rapport commun à la commission de la culture, de la science et de l'éducation à Paris le 18 mars 2011. Le présent exposé des motifs s'appuie largement sur ce rapport et je tiens à remercier chaleureusement ses auteurs.

5. Le 18 mars 2011, la commission a également entendu sur ce thème Mme de Terwangne et M. Colin, ainsi que Mme Pozzo di Borgo, qui s'exprimait au nom du Comité consultatif de la Convention no 108, M. Michael Donohue, analyste principal des politiques, de la sécurité de l'information et de la protection des renseignements personnels de l'OCDE, et M. Olivier Matter, juriste au Services des affaires européennes et internationales (CNIL), Paris. Les présentations faites pendant l'audition ont enrichi le présent rapport.

6. Les représentants de la Commission européenne et de la Chambre de commerce internationale n'ont pas pu assister à l'audition du 18 mars 2011. J'ai donc envoyé à ces deux institutions l'avant-projet de résolution afin qu'elles soumettent leurs observations.

7. Le commissaire à la protection des données du Conseil de l'Europe, le M. Karel Neuwirt, a également donné un avis sur le projet de rapport. Je le remercie de son avis positif et j'ai tenu compte de ses propositions dans mon rapport final.

8. Compte tenu des initiatives internationales ambitieuses lancées par des autorités indépendantes de protection des données, j'ai envoyé l'avant-projet de résolution à la Commission nationale de l'informatique et des libertés (CNIL, Paris) et àl'Institut fédéral d'accès à l'information et de protection des données de Mexico, qui accueillera en 2011 la Conférence des commissaires à la vie privée et à la protection des données.

9. Je remercie tous ceux qui m'ont aidée avec le présent rapport. J'espère qu'il contribuera à l'élaboration de normes communes sur la protection de la vie privée et des données à caractère personnel dans les pays européens et non européens, à l'ère du cyberespace.

---

4. Doc. 12021.
5. Pour une transcription des débats et des interventions qui ont eu lieu lors du forum ouvert, consulter: www.intgovforum.org/cms/2010-igf-vilnius/transcripts/646-1

1.2. Concepts de base

10. Le développement spectaculaire des technologies de l'information et de la communication (TIC) offre de grandes possibilités et de nombreux avantages. Le recours aux réseaux de communication et en particulier à l'internet a permis le déploiement de services jusqu'alors inimaginables, tout en accroissant l'efficacité et l'accessibilité des services classiques.

11. L'utilisation de ces technologies présente toutefois aussi de nouveaux dangers pour la vie privée et les libertés individuelles. Données recueillies à l'insu des personnes, données réutilisées pour des finalités inavouées, données conservées des mois, voire des années, données transmises à des tiers, données confidentielles diffusées: la réalité concernant le sort des données à caractère personnel sur l'internet a bien des faces noires. Les individus faisant usage du réseau et de toute la variété de services en ligne existant désormais perdent dans une grande mesure la maîtrise de leurs données. Ils ne savent pas ce qui est fait de leurs données, ils ne peuvent contrôler à distance qui y accède. Une série d'acteurs de l'internet et des nouveaux médias, en revanche, connaissent leurs goûts, leurs centres d'intérêt, leurs mouvements, les endroits et les personnes qu'ils fréquentent, etc. Cette réalité met en cause le droit au respect de la vie privée ainsi que le droit à la protection des données.

12. La vie privée, dans ce contexte, ne doit pas se comprendre de façon traditionnelle comme une sphère intime à protéger, contenant un ensemble d'informations privées, voire confidentielles, que l'on souhaite garder cachées, mais plutôt comme le droit à l'autodétermination, à l'autonomie et à la capacité de chacun de faire des choix existentiels[6]. Il s'agit ici, plus précisément, de l'autodétermination informationnelle, c'est-à-dire du droit de chacun «de savoir ce que l'on sait de lui», de connaître les informations stockées le concernant, de contrôler la manière dont elles sont communiquées et d'en empêcher toute violation abusive. La vie privée ne se réduit donc pas à une quête de confidentialité; ce qui est en jeu est la maîtrise par chacun de son image informationnelle.

13. La protection des données est une émanation du droit au respect de la vie privée pris dans la dimension de droit à l'autodétermination qui y est liée. C'est le droit pour chacun de contrôler ses propres données, qu'elles soient privées, publiques ou professionnelles.

2. Protection de la vie privée et des données personnelles en Europe

2.1. Normes juridiques

14. La présente section examine les textes juridiques contraignants adoptés au niveau du Conseil de l'Europe. Il est indiqué ensuite que le Pacte international relatif aux droits civils et politiques (PIDCP) est le seul instrument universel contraignant en matière de vie privée. Enfin, les dispositions de l'Union européenne sont étudiées dans la mesure où 27 Etats membres du Conseil de l'Europe sur 47 sont aussi des Etats membres de l'Union européenne. La même démarche est utilisée à l'égard de la liste des normes de politique figurant ci-dessous.

2.1.1. Article 8 de la Convention européenne des droits de l'homme

15. L'article 8 de la Convention européenne des droits de l'homme (STE no 5, ci-après «la Convention») garantit à chacun le droit au respect de sa vie privée et familiale. Des exceptions à ce droit sont admises pourvu qu'elles soient prévues par la loi et qu'elles soient nécessaires dans une société démocratique (c'est-à-dire qu'elles respectent le principe de proportionnalité tel que précisé par la jurisprudence de la Cour européenne des droits de l'homme («la Cour») pour sauvegarder les intérêts légitimes figurant dans la liste de l'article 8, paragraphe 2.

16. La Cour a expressément élargi le champ de la vie privée à celui de la protection des données. Elle a ainsi signalé que la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée consacré par l'article 8. Pour la Cour, l'article 8 impose que le droit interne ménage des garanties appropriées pour empêcher toute utilisation impropre et abusive de données à caractère personnel. La législation nationale doit également garantir que les données sont pertinentes et non

6. Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 de la Convention européenne des droits de l'homme, voir Evans c. Royaume-Uni, Requête no 6339/05, arrêt du 7 mars 2006 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007); Tysiac c. Pologne, Requête no 5410/03, arrêt du 20 mars 2007; Daroczy c. Hongrie, Requête no 44378/05, arrêt du 1er juillet 2008.

excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles ne sont conservées sous une forme permettant l'identification des personnes que pendant la durée nécessaire aux finalités pour lesquelles elles sont enregistrées[7].

2.1.2. Convention no 108

17. Née du souci de renforcer la protection de la vie privée et des autres droits de l'individu face aux développements des technologies de l'information, la Convention no 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été adoptée le 28 janvier 1981.

18. Cette convention contient les principes de base de la protection des données. Ces principes ont été repris dans la plupart des textes nationaux et internationaux en la matière et sont toujours d'actualité aujourd'hui, même s'ils nécessitent sans doute certains compléments. Ces principes sont les suivants:

– principe de loyauté et licéité de la collecte;

– principe de finalité (données enregistrées pour des finalités déterminées et légitimes et pas utilisées de manière incompatible avec ces finalités);

– principe de qualité des données (pertinentes, adéquates, à jour, conservées pour une durée limitée);

– régime spécifique réservé aux données sensibles;

– exigence de sécurité;

– droits d'accès, de rectification et de recours;

– possibilité de dérogations au nom d'intérêts publics ou privés prépondérants.

19. En 2001, un protocole additionnel portant sur les autorités de contrôle et les flux transfrontières de données (STE no 181) est venu compléter la Convention no 108.

20. Le comité consultatif établi dans le cadre de la Convention no 108 examine actuellement les lacunes juridiques éventuelles de la convention résultant des progrès technologiques rapides accomplis dans le monde des technologies de l'information et de la communication (TIC). Le rapport analytique préparé pour le comité consultatif par M. Jean-Marc Dinant, Mme de Terwangne et M. Jean-Philippe Moiny, de l'université de Namur (Belgique) est centré sur les défis technologiques que posent la géolocalisation, les cookies et la traçabilité, et les met en relation avec les normes juridiques visées par la Convention no 108[8].

21. Le comité consultatif a également poursuivi une consultation publique sur la modernisation possible de la Convention no 108 jusqu'en mars 2011.

2.1.3. Convention sur la cybercriminalité

22. La Convention sur la cybercriminalité (STE no 185), adoptée le 23 novembre 2001, a été élaborée par le Conseil de l'Europe, mais elle est ouverte à la signature de tous les Etats dans le monde[9]. Elle impose aux Etats signataires d'ériger en infraction pénale le fait de porter atteinte à la confidentialité des données, via l'accès non autorisé ou l'interception illégale de données, ou le fait de porter atteinte à l'intégrité des données, en les altérant ou en les supprimant, ou à l'intégrité du système. Les Etats parties doivent aussi sanctionner pénalement les faux informatiques et les fraudes informatiques, pour lutter contre les manipulations de données malintentionnées.

23. Par ailleurs, les parties doivent permettre à leurs autorités d'imposer la conservation rapide des données, y compris les données de trafic, afin d'en disposer pour des enquêtes. Un dispositif d'entraide entre parties permet de faire conserver et d'obtenir la divulgation de données par un autre Etat signataire de la convention.

7. S. et Marper c. Royaume-Uni, Requêtes nos 30562/04 et 30566/04, arrêt du 4 décembre 2008, paragraphe 103; également Rotaru c. Roumanie, Requête no 28341/95, arrêt du 4 mai 2000, paragraphe 55; M.S. c. Suède, Requête no 20837/92arrêt du 27 aout 1997.

8. .http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_09%20FINAL.pdf.

9. Elle a ainsi été signée par les Etats-Unis (qui l'a aussi ratifiée), le Canada, le Japon et l'Afrique du Sud.

2.1.4. Convention sur les droits de l'homme et la biomédecine

24. Les données à caractère personnel relatives à la santé font partie des données les plus sensibles sur le plan personnel. La protection de la vie privée et des données à caractère personnel est donc réglementée dans l'article 10 de la Convention sur les droits de l'homme et la biomédecine (STE no 164) et l'article 16 du Protocole additionnel à cette convention relatif aux tests génétiques à des fins médicales (STCE no 203).

25. Le droit de chacun à la protection des données à caractère personnel relatives à la santé doit inclure le droit d'être informé de toute collecte et traitement de ces données et d'y consentir ou non.

2.1.5. Article 17 du Pacte international relatif aux droits civils et politiques

26. L'article 17 du Pacte international relatif aux droits civils et politiques, signé à New York le 16 décembre 1966, stipule que «1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation; 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes». Cette disposition est la seule disposition contraignante qui protège la vie privée à un niveau universel.

2.1.6. Articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

27. Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte des droits fondamentaux de l'Union européenne[10] est juridiquement contraignante. Si l'article 7 de ce texte consacre classiquement la protection du droit au respect de la vie privée, l'article 8 présente l'originalité de garantir au sein d'un catalogue général de droits fondamentaux un droit autonome à la protection des données à caractère personnel. Cet article 8 dispose que toute personne a droit à la protection des données à caractère personnel la concernant; que les données doivent être traitées loyalement, à des fins déterminées, sur la base d'un fondement légitime (consentement ou autre fondement prévu par la loi); et que toute personne a un droit d'accès et de rectification de ses données. Le respect de ces principes doit être soumis au contrôle d'une autorité indépendante.

2.1.7. Directive 95/46/CE de l'Union européenne sur la protection des données

28. La Directive 95/46/CE 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[11] a repris, en les détaillant et les précisant, les principes contenus dans la Convention no 108. Elle présente toutefois un régime de protection enrichi sur plus d'un point. Elle a établi les critères qui rendent le traitement des données légitime. Le catalogue des droits reconnus à la personne concernée est étoffé. Le droit d'accès englobe le droit de connaître l'origine des données et la logique qui sous-tend le traitement des données. Le droit de s'opposer au traitement de ses données et le droit de ne pas être soumis à une décision entièrement automatisée sont consacrés. En outre, un devoir d'information est mis à charge du responsable du traitement des données. Actuellement, une réforme de la législation de l'Union européenne concernant la protection des données est en cours.

2.1.8. Directive 2002/58/CE de l'Union européenne sur la vie privée et les communications électroniques

29. La Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[12]est une directive spécifique qui s'ajoute à la Directive générale (95/46/CE) pour réglementer la protection des données dans le secteur des communications électroniques. Elle proclame l'obligation de confidentialité des communications électroniques ainsi que des données de trafic et des données de localisation, moyennant certaines exceptions. Elle instaure un devoir de sécurité des données, allant désormais de pair avec l'obligation d'informer des «violations de données» graves survenues. Cette obligation ne pèse cependant que sur les fournisseurs de services de communications électroniques accessibles au public. Ce texte règle aussi le recours aux cookies et l'envoi de communications non sollicitées (spam).

10. Voir http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF.
11. J.O.U.E., L 281, du 23 novembre 1995, p. 31-50.
12. J.O.U.E., L 201, du 31 juillet 2002, p. 37-47.

2.1.9. Directive 2006/24/CE de l'Union européenne sur la conservation des données

30. La Directive 2006/24/CE du 15 mars 2006 exige que les fournisseurs de services de communication (internet, téléphonie fixe et mobile, télécopie) conservent systématiquement les données concernant la localisation et le trafic des communications pendant une durée de six mois à deux ans[13]. Cette directive est en train d'être modifiée.

31. La conservation des données et l'accès à ces données par les autorités de police sont devenus un aspect politiquement important de la lutte contre la criminalité et le terrorisme. A cet égard, la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE no 198) et la Convention sur la cybercriminalité pourraient servir de références juridiques, ainsi que la Convention concernant l'assistance administrative mutuelle en matière fiscale (STE n o 127 et STCE n o 208).

2.2. Normes en matière d'élaboration de politiques

Résolution 428 (1970) de l'Assemblée portant déclaration sur les moyens de communication de masse et les droits de l'homme

32. Dans sa Résolution 428 (1970) portant déclaration sur les moyens de communication de masse et les droits de l'homme, l'Assemblée parlementaire a établi il y a déjà plus de quarante ans que «lorsque des banques régionales, nationales ou internationales de données informatiques sont instituées, l'individu ne doit pas être rendu totalement vulnérable par l'accumulation d'informations concernant sa vie privée. Ces centres doivent enregistrer uniquement le minimum de renseignements nécessaires».

33. Cette résolution donnait suite à la Recommandation 509 (1968) relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes, qui appelait le Comité des Ministres à«étudier et faire rapport sur la question de savoir, au regard de l'article 8 de la Convention [européenne] des droits de l'homme, si la législation nationale des Etats membres assure une protection adéquate du droit à la vie privée contre des violations qui pourraient être commises par l'utilisation de méthodes techniques et scientifiques modernes».

34. La résolution a été adoptée conjointement avec la Recommandation 582 (1970) relative aux moyens de communication de masse et droits de l'homme, qui renouvelait le premier appel en recommandant au Comité des Ministres d'envisager la «mise au point d'une interprétation commune du droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme, par la conclusion d'un protocole ou de tout autre instrument, de façon à préciser que l'exercice de ce droit est effectivement protégé contre toute ingérence non seulement des pouvoirs publics, mais aussi des personnes privées ou des moyens de communication de masse».

Résolution 1165 (1998) de l'Assemblée sur le droit au respect de la vie privée

35. Dans sa «Déclaration sur les moyens de communication de masse et les droits de l'homme» contenue dans la Résolution 428 (1970), l'Assemblée avait défini le droit au respect de la vie privée comme «le droit de mener sa vie comme on l'entend avec un minimum d'ingérence». Près de trente ans plus tard, l'Assemblée a précisé dans la Résolution 1165 (1998) que «pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition le droit de contrôler ses propres données».

36. La résolution de 1998 contient des lignes directrices destinées à compléter les régimes nationaux de protection de la vie privée, portant sur les différentes actions en justice et sanctions à mettre à disposition des personnes ayant subi des atteintes à leur vie privée.

Résolution 1797 (2011) de l'Assemblée sur la nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme

37. L'Assemblée a récemment adopté une Résolution 1797 (2011) sur la nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme, qui invite en particulier les Etats membres à «promouvoir le principe de proportionnalité en matière d'utilisation de données biométriques, notamment en limitant au strict nécessaire l'évaluation, le traitement et le stockage de ces données, en

13. J.O.U.E., L 105, du 13 avril 2006, p. 54-63.

d'autres termes, en limitant ces processus aux cas où le gain en termes de sécurité ou de protection de la santé publique ou des droits d'autrui serait plus important qu'une éventuelle ingérence dans les droits de l'homme, et si le recours à d'autres techniques moins intrusives est insuffisant».

Recommandation (73) 22 du Comité des Ministres relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé

38. Le Comité des Ministres a élaboré le premier ensemble de principes politiques dans sa Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé[14]. En adoptant cette résolution le 26 septembre 1973, le Comité des Ministres a considéré qu'il était urgent, en attendant l'élaboration éventuelle d'un accord international, de prendre des mesures pour empêcher que d'autres divergences n'apparaissent entre les lois des Etats membres dans ce domaine.

39. La Résolution (73) 22 définissait notamment ceci: «les informations concernant l'intimité des personnes ou celles pouvant être à la source de discrimination ne doivent pas, en règle générale, être enregistrées, ou du moins diffusées; des règles devront être établies pour déterminer la période de temps au-delà de laquelle certaines catégories d'informations ne pourront plus être conservées ou utilisées; les informations ne peuvent, sans autorisation appropriée, être utilisées à d'autres fins que celles pour lesquelles elles ont été enregistrées, ni communiquées à des tiers; en règle générale, la personne concernée a le droit de connaître les informations enregistrées sur elle, la fin pour laquelle les informations ont été stockées et les communications effectuées; toute diligence doit être faite pour corriger les informations inexactes et pour effacer les informations périmées ou obtenues de façon illicite; les banques de données électroniques doivent être équipées de systèmes de sécurité empêchant les personnes n'ayant pas le droit d'obtenir les informations d'y avoir accès et permettant de détecter les détournements d'informations, intentionnels ou non». De telles normes semblent encore pertinentes, même avec le niveau de développement des TIC aujourd'hui.

Résolution (74) 29 du Comité des Ministres relative à la protection des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public

40. La Résolution (73) 22 a été complétée un an plus tard par la Résolution (74) 29 relative à la protection des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public. Outre un ensemble de normes comparables, la Résolution (74) 29 disposait ceci: «[p]articulièrement lorsque des banques de données électroniques traitent des informations concernant l'intimité de la vie privée des personnes, ou lorsque le traitement des informations peut être à l'origine de discriminations; a) leur création doit être prévue par la loi ou par une réglementation spéciale ou leur existence doit être rendue publique dans une déclaration ou un document, en conformité avec le système juridique de chaque Etat membre; b) ces loi, réglementation, déclaration ou document doivent préciser la finalité de l'enregistrement et de l'utilisation de telles informations ainsi que les conditions dans lesquelles elles peuvent être communiquées à l'intérieur du secteur public ou à des personnes ou organismes privés; c) les informations enregistrées ne doivent pas être utilisées à d'autres fins que celles qui ont été définies, à moins qu'une dérogation ne soit expressément autorisée par la loi ou accordée par une autorité compétente ou que les règles régissant l'utilisation de la banque de données électroniques ne soient modifiées».

Recommandation no R (99) 5 du Comité des Ministres sur la protection de la vie privée sur internet

41. La Recommandation no R (99) 5 s'adresse aux utilisateurs et aux fournisseurs de services sur l'internet. Elle contient des Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les «inforoutes», destinées à être intégrées dans des codes de conduite. Ces lignes directrices énoncent les principes d'une conduite loyale à observer en matière de protection de la vie privée et des données lors des communications et échanges sur l'internet.

Recommandation CM/Rec(2010)13 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

14. Voir https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2.

42. Adoptée le 23 novembre 2010, la Recommandation CM/Rec(2010)13 propose un encadrement du phénomène très répandu du profilage (voir les sections 3.2 et 4.2 ci-dessous). L'annexe à la recommandation contient les principes devant conduire à un profilage loyal et licite. Une liste des cas dans lesquels le profilage est licite est établie. Le responsable est tenu de limiter les risques d'erreurs, d'adopter des mesures de sécurité et d'informer les personnes concernées de ses activités de profilage. Sauf exceptions, les individus ont le droit d'accéder aux données, de les corriger, de connaître le but du profilage ainsi que la logique utilisée pour leur attribuer un profil, et enfin, de s'opposer à l'utilisation de leurs données ou à une décision prise sur la seule base du profilage.

Résolution no 3 de la Conférence des ministres européens de la Justice sur la protection des données et la vie privée au troisième millénaire

43. Dans la Résolution no 3, adoptée le 26 novembre 2010 lors de leur 30e conférence ministérielle à Istanbul, les ministres de la Justice du Conseil de l'Europe marquent leur soutien à la modernisation de la Convention n o 108 afin de trouver les solutions pour garantir la protection des droits de l'individu face aux nouveaux défis de la technologie et de la mondialisation de l'information. Cette modernisation devrait répondre aux préoccupations exprimées par les ministres sur les questions de transparence, d'exercice effectif des droits, de violation de la sécurité des données, de compétence territoriale et de droit applicable en présence de relations virtuelles et transfrontières (dans le*cloud computing* et les réseaux sociaux, par exemple), et de responsabilité.

44. Les ministres signalent que la Convention n o 108 est à ce jour le seul instrument juridiquement contraignant de portée potentiellement universelle en la matière. Ce texte pourrait donc devenir l'instrument universel réclamé par les autorités nationales de protection des données. Les ministres invitent en conséquence les acteurs en marge du Conseil de l'Europe à participer au processus de modernisation.

Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par l'Assemblée générale des Nations Unies le 14 décembre 1990

45. L'Assemblée générale des Nations Unies a adopté le 14 décembre 1990 des principes directeurs concernant les fichiers informatisés contenant des données à caractère personnel[15].

46. Ces principes directeurs sont la seule norme politique établie par les Nations Unies depuis l'entrée en vigueur de l'article 17 du PIDCP. Ils énoncent que les données concernant les personnes ne doivent pas être utilisées «à des fins contraires aux buts et aux principes de la Charte des Nations Unies».

Lignes directrices de l'OCDE de 1980 sur la protection de la vie privée et les flux transfrontières de données à caractère personnel

47. Les lignes directrices de l'OCDE de 1980[16] contiennent des «principes d'information équitables». Ces principes de base de la protection des données sont presque identiques à ceux contenus dans la Convention no 108. Mais à la différence de ces derniers, ils ne sont pas juridiquement contraignants.

48. L'OCDE examine actuellement ses lignes directrices sur la protection des données en vue de les moderniser. La plupart des Etats membres de l'OCDE sont juridiquement contraints par la législation de l'Union européenne et/ou la Convention n o 108.

Résolution de Madrid de 2009 adoptée par les commissaires à la protection des données et à la vie privée

49. La Résolution de Madrid[17] de 2009 est issue d'un travail conjoint des autorités de protection des données de 50 pays sous la houlette de l'Agence espagnole de la protection des données. Elle vise à offrir un modèle reprenant les standards universels de la protection des données. Elle réalise donc l'intégration des valeurs et principes de protection des données garantis sur les cinq continents.

---

15. http://ec.europa.eu/justice/policies/privacy/instruments/un_en.htm.
16. www.oecd.org/document/18/0,3746,en_2649_33725_42177095_1_1_1_1,00.html.
17. Proposition conjointe visant à établir un projet de normes internationales sur la vie privée au regard du traitement des données à caractère personnel: www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.

50. Outre les aspects classiques de la protection des données, cette résolution contient des éléments nouveaux, par exemple des mesures proactives (procédures visant à prévenir et détecter les failles de sécurité, désignation d'un correspondant à la protection des données, réalisation d'études d'impact pour la vie privée, etc.) ainsi que le principe de responsabilité qui prévoit l'obligation de mettre en place des mécanismes internes permettant de démontrer que le responsable s'est conformé aux règles de protection.

Résolution de Jérusalem de 2010 adoptée par les commissaires à la protection des données et à la vie privée

51. A leur 32e Conférence internationale, organisée à Jérusalem du 27 au 29 octobre 2010, les autorités de protection des données ont adopté une résolution appelant à l'organisation d'une conférence intergouvernementale en vue d'élaborer un instrument international contraignant sur la vie privée et la protection des données à caractère personnel[18].

52. Donnant suite à cette initiative, les ministres de la Justice du Conseil de l'Europe ont adopté, lors de leur 30e conférence, la Résolution n o 3 sur la protection des données et la vie privée au troisième millénaire (voir ci-dessus), qui invitait les Etats non européens à adhérer à la Convention n o 108 et appuyait sa modernisation.

3. Défis technologiques pour la vie privée et la protection des données

53. La puissance de calcul et de stockage toujours plus importante, et la connectivité toujours plus étendue rendent possible le développement de nouvelles technologies et applications qui constituent de véritables défis pour la vie privée et la protection des données. Elles impliquent bien souvent une collecte massive de données personnelles sur les citoyens, acheteurs en ligne, utilisateurs de réseaux sociaux, etc., parfois à leur insu; l'utilisation de plus en plus répandue d'identifiants permettant de lier un utilisateur à ses actions, sa position géographique ou ses données (tels l'adresse IP, l'identifiant présent sur un tag RFID, un numéro de session dans un cookie). De plus, ces informations peuvent être analysées et corrélées pour en déduire d'autres, à des fins de profilage par exemple. Enfin, le stockage et la diffusion des informations collectées ou inférées échappent de plus en plus fréquemment au contrôle de la personne concernée, qui se retrouve impuissante devant l'utilisation parfois abusive qui en est faite.

54. Les conséquences en sont des risques accrus de fuites d'information et de traçage des personnes, mettant ainsi à mal la vie privée de celles-ci. Il est donc nécessaire de passer en revue une série de technologies émergentes ou en mutation, en décrivant d'une manière générale leurs applications et leur fonctionnement, mais aussi les menaces potentielles qu'elles présentent pour la vie privée et la protection des données.

55. La Commission européenne avait commandé une étude comparative sur les différentes approches relatives aux défis que représentent les progrès technologiques pour la vie privée. Cette étude, qui a été présentée le 20 janvier 2010 par ses auteurs, LRDP Kantor Ltd. (Cambridge/London/Oxford), proposait de moderniser la Directive 95/46/CE de l'Union européenne 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[19].

3.1. Convergence des moyens de communication

56. L'évolution des systèmes de communication et des services de diffusion et de partage d'information conduit à une convergence de plus en plus importante entre ces différents systèmes, avec pour conséquence un manque de plus en plus important de transparence quant aux véritables outils utilisés, et surtout une perte de contrôle de la diffusion de l'information qui circule, est agrégée, remise en forme ou réexpédiée.

57. Ainsi, le téléphone, doté d'une puissance de calcul et de stockage, devient par là «intelligent» (smartphones); l'ordinateur permet de téléphoner; la vidéoconférence est disponible sur des baladeurs mp3; un numéro de télécopie est en fait une façade pour une adresse électronique; les appels vers un téléphone mobile peuvent être redirigés vers un poste fixe, avant d'échouer sur la boîte vocale d'un service de type VoIP (Voice Over IP – téléphonie sur réseau IP) consultée sur un PC. Ces exemples montrent à quel point il devient très compliqué pour un utilisateur de déterminer le type de moyen de communication utilisé, et surtout où vont et d'où proviennent les informations envoyées ou reçues.

---

18. www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26499/ResoutiononInternationalConference.pdf.
19. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

58. Il convient de mentionner également à ce sujet des développements tels que «Outlook Social Connector» de Microsoft, qui permet aux destinataires d'un courriel d'obtenir le statut Facebook de l'expéditeur. Cela montre la confusion de plus en plus grande entre des sphères qui jusqu'ici étaient clairement distinctes, et les risques de diffusion d'information non souhaitée que cela permet.

3.2. Exemples de nouvelles technologies

– Géolocalisation

Traçabilité des utilisateurs

59. Contrairement à ce que l'on pense, la navigation sur l'internet laisse bien davantage de traces que déambuler et agir dans la vie réelle. Les actions que l'on effectue sur l'internet laissent entre les mains de différentes personnes des traces de ce que l'on a fait (adresse IP, fournisseur d'accès, page d'où l'on vient, historique de la navigation, etc.). Les outils comme l'adressage IPv6 et les cookies (voir ci-dessous) permettent d'individualiser un ordinateur et dès lors son utilisateur. A l'inverse de ce qui se passe dans le monde physique réel, il n'est pas question de se promener sur les inforoutes, d'entrer dans les magasins virtuels, de lire le journal, d'être intéressé par une annonce commerciale, sans que cela se sache. On ne peut manquer de s'interroger sur cette transparence permanente qui ne serait sans doute pas tolérée dans le monde réel.

Adressage IPv6

60. En raison de la prolifération des systèmes connectés à l'internet, la plage d'adresses définie par la norme IPv4[20] est épuisée, ce qui menace l'expansion d'internet. La norme IPv6, créée pour répondre aux nouveaux besoins d'adressage, permet d'obtenir un très grand nombre d'adresses distinctes[21]. A titre d'illustration, IPv6 donnerait à chaque individu sur terre la possibilité de disposer de plusieurs dizaines de milliards d'adresses pour son usage personnel.

61. L'assignation d'une adresse IPv6 à un équipement peut être réalisée de différentes manières, dont l'une utilise l'adresse physique (adresse MAC) de l'appareil pour générer l'adresse IPv6, ce qui permet alors de lier le trafic à une machine, voire de conduire à une personne. D'autres modes permettent d'éviter cette situation, en générant des adresses de manière pseudo-aléatoire ou en recourant à un serveur d'adresses qui les assigne de manière automatique[22].

62. Le caractère identifiant ou non de l'adresse IPv6 dépendra donc soit des paramètres de configuration par défaut du système utilisé, soit de la compétence de l'utilisateur.

Cookies

63. Le mécanisme des cookies est défini par le protocole de navigation web (http) et permet à un serveur web de transmettre au navigateur de l'internaute une série d'informations que celui-ci lui retournera lors des visites ultérieures (vers ce site uniquement). Le cookie a une durée de vie limitée, soit liée à la fermeture du navigateur, soit à une date d'expiration. Les cookies sont donc stockés localement par le navigateur, en général sur le disque dur de l'utilisateur.

64. Les cookies sont utilisés par les serveurs web à des fins de gestion de session et de personnalisation, mais ils peuvent aussi servir comme moyen de traçage. De plus, il faut noter que lors de la visite d'un site, le navigateur peut recevoir des cookies provenant de sites tiers, cela étant dû à l'inclusion dans le site consulté originellement de contenu provenant de ces sites tiers. Cette technique est fréquemment utilisée pour la mesure d'audience ou le profilage publicitaire.

---

20. IPv4 définit un format d'adresse sur 4 bytes, représentant chacun une valeur entre 0 et 255, soit 232 ≃ 4,109 adresses possibles.
21. IPv6 utilise un format d'adresse sur 16 octets, représentant chacun une valeur entre 0 et 255, soit 2128 ≃ 256,1036 adresses possibles.
22. Ce mécanisme utilise le protocole DHCP.

65. Bien que les navigateurs les plus répandus permettent aux internautes de gérer voire de bloquer les cookies, ces fonctions sont rarement utilisées, soit par méconnaissance, soit plus simplement parce que le blocage des cookies rendrait la navigation internet impraticable.

Réseaux de distribution intelligents

66. On assiste à une évolution des réseaux de distribution d'énergie vers une forme intelligente (réseau intelligent) dans laquelle sont incorporées des technologies informatiques afin d'optimiser la production et la distribution, l'objectif étant d'ajuster au mieux la production et la consommation, conduisant ainsi à des économies d'énergie, l'évitement de pannes de courant, etc. Un réseau intelligent est composé de compteurs intelligents équipés de capteurs et liés, via un réseau, à un système qui collecte, agrège et analyse les données de consommation.

67. Les compteurs intelligents transmettent à l'opérateur des données relatives à la consommation en temps réel, ce qui permet de déterminer le profil de l'utilisateur, son absence ou sa présence dans le bâtiment, l'utilisation d'appareils possédant une «signature énergétique», etc.

68. De plus, à l'intérieur même du bâtiment, des appareils peuvent aussi être connectés au compteur intelligent, l'informant de la consommation instantanée, mais aussi lui permettant d'agir sur celle-ci, par exemple en adaptant automatiquement la température d'un thermostat ou en désactivant l'air conditionné lors d'un pic de consommation.

69. On assiste là encore à une collecte massive d'informations pouvant être liées à une personne ou un groupe de personnes, permettant d'en déduire des caractéristiques et des comportements de manière très ciblée. Lorsqu'en plus ces informations sont collectées par des tiers, comme c'est le cas pour le système PowerMeter[23] de Google, le risque de les voir diffusées sans contrôle est encore plus grand.

– RFID et l'Internet des objets

70. La technologie RFID (Radio-Frequency Identification) est une technique d'identification qui se base sur trois composants:

– l'étiquette, ou tag, qui est collée ou intégrée à l'objet à identifier;

– le lecteur, utilisé pour interroger le tag lorsque celui-ci est à sa portée;

– le système d'information, qui reçoit l'information du lecteur et la traite.

71. Le tag est composé d'une antenne et d'une puce électronique, qui contient, au minimum, un identifiant. Lorsque le tag est interrogé par un lecteur (par l'utilisation d'ondes magnétiques), il transmet son identifiant au lecteur. La structure du tag, très simple, autorise une production de masse à un coût qui permet une utilisation à grande échelle, soit quelques centimes d'euro[24]. La lecture du tag ne nécessite pas de contact entre celui-ci et le lecteur; en fonction du type de tag, la distance de lecture peut varier entre quelques centimètres ou quelques dizaines de centimètres, voire au-delà.

72. Les tags RFID sont utilisés dans la gestion des stocks et de l'approvisionnement, pour les péages routiers, dans la grande distribution pour la gestion de l'inventaire, des caisses ou du service après-vente, dans les aéroports pour le suivi des bagages ou comme moyen de marquage des animaux. Dans certains cas, les tags peuvent être implantés chez des êtres humains, par exemple pour assurer la sécurité d'enfants ou de personnes âgées, ou, dans un registre plus léger, pour surveiller l'accès ou gérer les commandes de consommations dans une discothèque. L'identifiant étant spécifique à un tag, la lecture de celui-ci permet donc de suivre ses déplacements, d'après la position du lecteur, et donc ceux de l'objet ou de la personne qui le porte. La lecture se faisant à distance, l'utilisateur n'est pas nécessairement conscient de celle-ci, ce qui peut conduire à des fuites d'information ou un traçage à son insu. L'interrogation simultanée d'un grand nombre de tags permet d'identifier très rapidement les objets ou personnes marquées dans un environnement proche, et donc là aussi aboutir à un profilage du porteur.

---

23. Google PowerMeter est un système permettant à un utilisateur de visualiser sur le web sa consommation énergétique, ce système étant alimenté à partir du compteur intelligent installé chez l'utilisateur. L'accès à cette information est normalement réservé à l'utilisateur en question.

24. Il convient de noter qu'un tag peut être plus perfectionné. En effet, il peut contenir d'autres informations que l'identificateur et posséder sa propre batterie afin d'être en mesure de transmettre sur de plus longues distances ou de jouer le rôle d'un capteur, par exemple.

73. Différentes solutions techniques existent (et d'autres continuent d'être développées) qui permettent de limiter les possibilités d'utilisation malveillante des technologies RFID. Mais bien souvent leur mise en œuvre fait augmenter significativement le coût de fabrication, rendant difficile leur utilisation à large échelle. Récemment, le groupe de travail «Article 29» sur la protection des données de l'Union européenne a approuvé un cadre d'évaluation de l'impact sur la vie privée pour les demandes RFID[25].

74. L'Internet des objets (Internet of Things) pousse l'idée de l'internet et de l'identification un (grand) pas plus loin, en décrivant un monde où tout est interconnecté: les personnes, mais aussi les objets. L'internet sort donc du monde strictement virtuel pour intégrer les objets du monde réel, physique, en utilisant des technologies telles que la RFID, les communications sans fil à courte portée (NFC – Near Field Communication, ou Communication en champ proche), la géolocalisation et les réseaux de capteurs. Dans ce scénario, les objets connectés agissent avec un haut degré d'autonomie, capables d'acquérir et de transmettre des informations collectées au travers de capteurs, de les traiter, et d'interagir avec les utilisateurs et leur environnement.

75. Bien que l'Internet des objets soit encore une discipline récente, dont les utilisations scientifiques et commerciales en restent encore à leurs balbutiements, il est cependant évident qu'il se base sur des collectes et des traitements massifs d'information, pour la plupart pouvant être liées directement ou indirectement à des individus, et par là même, menacer leur vie privée.

Robots d'indexation

76. Un robot d'indexation (*webcrawler* ou *webspider*) est un logiciel écrit pour explorer le web de manière automatique, afin d'indexer le contenu visité et alimenter ainsi les moteurs de recherche pour permettre une recherche plus efficace et donc un accès plus aisé à l'information. Il fonctionne par analyse des pages visitées, en suivant récursivement les hyperliens.

77. Certains robots malveillants analysent les pages pour en extraire les adresses de courrier électronique afin de constituer des listes de diffusion pour l'envoi de messages intempestifs (spams). D'autres peuvent aussi parcourir des pages, afin d'agréger et de corréler les informations collectées et en inférer d'autres.

Données biométriques

78. Des moyens biométriques, c'est-à-dire liés à des caractéristiques physiologiques de l'individu telles que ses empreintes digitales, son empreinte rétinienne, son empreinte vocale ou son ADN, sont de plus en plus utilisés pour authentifier une personne (vérifier son identité), que ce soit dans le domaine des paiements électroniques, du contrôle aux frontières, du contrôle d'accès, la reconnaissance faciale, etc.

79. Les données biométriques doivent d'abord être collectées, avant de pouvoir être confrontées à celles fournies lors de l'authentification et ainsi valider celle-ci. Cela implique le stockage d'une grande quantité de données à caractère personnel, dont certaines, telles que l'ADN, sont une intrusion dans l'intimité de l'individu, y compris celle de son ascendance et de sa descendance.

80. L'Assemblée a adopté récemment la Résolution 1797 (2011) et la Recommandation 1960 (2011) sur la nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme. Ces textes visaient précisément la protection des données à caractère personnel et la vie privée.

Respect de la vie privée dès la conception

81. Le terme anglais «privacy by design», ou respect de la vie privée dès la conception, fait référence à un ensemble de principes élaborés pour être utilisés lors de la conception, du développement et de l'exploitation de systèmes d'information, afin de garantir que les dimensions «vie privée» et «protection des données» ont été correctement prises en compte dès la conception, et que dès lors ces systèmes sont en conformité avec les exigences légales et réglementaires en la matière.

82. Mme Ann Cavoukian, commissaire à l'information et la vie privée de la province d'Ontario (Canada), est à l'origine de cette initiative fondée sur le respect de l'utilisateur, la transparence à son égard pour ce qui concerne la collecte et le traitement des données, et le refus de compromis dans lesquels la vie privée serait sacrifiée au profit d'autres objectifs. Les principes de base sont le caractère proactif des mesures de sécurité, le fait que, par défaut, la protection des données est assurée, toute dérogation devant avoir l'approbation de

25. Voir http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_fr.pdf.

la personne concernée, le fait que la protection des données doit être considérée comme partie intégrante des fonctions du système d'information, plutôt qu'une fonctionnalité annexe, et qu'elle doit être maintenue tout au long du cycle de vie de l'information collectée.

83. Ces principes sont applicables aussi bien au domaine de la technologie de l'information, qu'à celui des pratiques métiers et de l'infrastructure physique. Un portail internet est consacré à cette approche[26], qui outre une présentation générale, démontre l'applicabilité de la démarche au travers de nombreux cas d'études, montrant ainsi qu'il est possible de concevoir des systèmes efficaces et répondre aux exigences-métier sans pour autant sacrifier la protection des données.

Cloud computing

84. Le *cloud computing* est un paradigme IT récent. Le terme fait référence à la fois aux services accédés et délivrés via l'internet, et aux systèmes d'information et à l'infrastructure matérielle et logicielle qui fournit ces services.

85. Le *cloud* permet une grande flexibilité dans la gestion et l'allocation des ressources, où le modèle d'investissement s'oriente plus vers un modèle de facturation à l'usage, ainsi qu'une grande souplesse dans l'intégration de services, de manière intra- ou interorganisationnelle, indépendamment de l'implantation géographique.

86. Les services de type *cloud* peuvent être offerts à différents niveaux; on distingue généralement trois modèles différents:

– les services offerts sont de type «infrastructure» (IaaS), soit principalement du matériel et du logiciel de base, ainsi que de la connectivité; la gestion de cette infrastructure est laissée au client;

– les services offerts prennent la forme d'une plate-forme opérationnelle (PaaS), composée de l'infrastructure, mais aussi de l'environnement logiciel permettant au client de développer ou d'exploiter ses propres applications; la gestion de l'ensemble est donc partagée entre le fournisseur de service et son client;

– le fournisseur offre ici une solution applicative complète à son client (SaaS), en prenant en charge à la fois l'infrastructure, mais aussi l'application. De tels services sont offerts par exemple par salesforce.com, pour la gestion commerciale, ou par Google, au travers de ses services mail, documents, agenda, etc.

87. Le *cloud computing* constitue donc une extension du périmètre de sécurité vers l'internet, où il est fort compliqué d'effectuer un contrôle efficace. Le stockage de ses données est confié par l'utilisateur à un tiers, le fournisseur de services, qui les héberge et les traite dans des conditions bien souvent inconnues de l'utilisateur. Cela nécessite une réelle relation de confiance entre l'utilisateur et le fournisseur de services. Cette confiance peut être renforcée par des garanties contractuelles. Les défis principaux se situent autour de la protection des données confiées au *cloud*, de la préservation de leur intégrité et du maintien d'un contrôle d'accès approprié.

Inspection en profondeur du trafic

88. L'information circulant sur un réseau est classiquement transmise sous forme de paquets, formés d'un en-tête et d'un corps; l'en-tête contient l'information nécessaire pour permettre aux équipements réseaux traversés de mener le paquet jusqu'à sa destination.

89. Le filtrage du trafic réseau, opéré principalement par des pare-feux *(firewalls)*, se base, pour autoriser ou non le transit, sur les informations de routage présentes dans l'en-tête des paquets, soit principalement l'origine et la destination du message. L'inspection en profondeur du trafic *(deep packet inspection)* se base en plus sur des critères de contenu, en analysant non seulement l'en-tête, mais aussi le corps du message, c'est-à-dire son contenu.

90. La technique est évidemment plus coûteuse en temps et en ressources. Elle permet d'améliorer la sécurité des systèmes d'information, en détectant et filtrant le contenu malicieux. Mais elle peut aussi être détournée à des fins de surveillance ou de censure.

26. Voir www.privacybydesign.ca/.

4. Défis liés à l'usage

4.1. Traitement de données

Par les autorités publiques

91. Le développement de l'«e-gouvernement» à partir de l'utilisation des TIC conduit à une organisation en réseau des autorités publiques. Cette évolution se base essentiellement sur le partage de données entre autorités, la création de fichiers de référence et de vastes entrepôts de données et l'interconnexion de bases de données autrefois indépendantes. Ce modèle suscite d'importantes interrogations relatives à la protection de la vie privée. Le modèle antérieur de l'administration «en silos», chaque entité disposant d'informations propres, isolées, destinées à réaliser la mission légale de l'entité, était présenté comme la garantie contre un Etat omniscient à l'égard duquel le citoyen serait totalement transparent. L'«obscurité pratique» était la clé de l'équilibre dans la relation administration-administrés. Cette garantie a disparu au nom de l'efficacité. On doit aujourd'hui impérativement poser la question de la maîtrise par chacun des informations collectées à son propos, de la transparence des échanges et de la proportionnalité des traitements.

92. Le recours aux identifiants uniques servant d'instruments d'interconnexion et d'accès transversal aux données d'un individu augmente encore les risques de perte de contrôle et de non-respect de la proportionnalité. Les inquiétudes face aux traitements de données personnelles par les autorités publiques sont accentuées par le fait que ces traitements servent de base à la prise de décisions telles l'octroi d'une pension, la reconnaissance d'un statut particulier, l'établissement de l'impôt, l'ouverture d'enquêtes pénales, etc.

93. Martin Scheinin, rapporteur spécial des Nations Unies pour la protection et la promotion des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, condamne, dans son rapport à la 13e session du Conseil des droits de l'homme de l'ONU, l'érosion de la vie privée du fait des mesures adoptées pour lutter contre le terrorisme[27]. De nombreux Etats ont considérablement élargi leurs pouvoirs en invoquant la sécurité nationale et la sûreté publique, notamment la surveillance ouverte ou secrète, l'interception des communications et le profilage des personnes.

94. La Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE no 205) s'efforce de trouver un équilibre entre le droit à l'information et la protection de la vie privée et des données à caractère personnel.

Par les entités commerciales

95. Les données personnelles représentent une valeur économique. Cette valeur est importante à trois niveaux:

– pour les fournisseurs de services internet car connaître le profil des internautes intéressés par les produits ou services et pouvoir détailler très précisément leur intérêt (pages web lues, liens cliqués, fréquence des visites, etc.) permet de configurer l'offre de manière optimale;

– pour les utilisateurs commerciaux des bases de données contenant des informations à caractère personnel, car la collecte de données tous azimuts permet de constituer de très riches bases de données exploitables et revendables pour des activités de communication et de publipostage;

– pour le fonctionnement réel du web, car la gratuité de la plupart des services offerts sur le web n'est que de façade. L'exposition publicitaire des utilisateurs finance l'offre. Le modèle économique repose sur le marketing. Celui-ci sera d'autant plus rentable que le profil des destinataires est précis et permet de cibler efficacement les messages publicitaires[28].

96. Dans ces trois schémas, la collecte et le croisement d'informations conduisant à dessiner les profils des utilisateurs deviennent des opérations cruciales. Ces opérations se font toutefois dans de trop nombreux cas à l'insu des personnes concernées. Elles impliquent souvent une utilisation des données au-delà des finalités originelles. Et la quantité des données collectées pose inévitablement la question de la proportionnalité. Est-il nécessaire ou tout simplement normal, par exemple, que les moteurs de recherche (comme Google)

27. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

28. Pour Google et Facebook, le profit tiré des activités de marketing opérées sur leurs sites s'élève annuellement à plusieurs milliards de dollars.

conservent durant des mois tous les mots introduits par une personne (individualisée grâce à un cookie) ? Cet ensemble de mots est le plus souvent incroyablement révélateur de ses centres d'intérêts, ses activités, ses projets, etc.

97. La Commission nationale de l'informatique et des libertés (CNIL) surveille et punit les violations de la vie privée et de la protection des données en France depuis 1974. Dans le passé, 90 % des cas traités par la CNIL étaient des violations commises par le secteur public. Désormais, c'est le secteur privé qui représente 90 % des cas. De 2005 à 2009, le nombre des cas a triplé. Dans sa décision 2011-35 du 17 mars 2011, la CNIL a prononcé une amende de 100 000 euros à l'encontre de Google-France pour avoir collecté et traité secrètement un grand nombre de données à caractère personnel résultant de ses réseaux Wi-Fi et des services Google Location Server pendant la captation d'images prises par des caméras mobiles pour les services Google Map et Google Street View[29].

Par les employeurs

98. Les TIC ont mis entre les mains des employeurs des outils de surveillance inimaginables autrefois. Les cartes magnétiques d'accès aux locaux disent à l'opérateur du réseau qui se trouve où et à quelle heure, alors que les clés classiques étaient muettes à ce sujet. Les réseaux de caméras permettent de surveiller les visiteurs aussi bien que le personnel. La surveillance du personnel s'effectue également par le contrôle de la navigation sur l'internet et l'usage du courrier électronique mis à la disposition des travailleurs. Pour les employés qui travaillent hors des murs de l'entreprise, les systèmes de localisation et de suivi géographique permettent de gérer à distance les flottes de taxis, les véhicules en panne ou les véhicules en circulation, et de surveiller leurs déplacements en temps réel.

99. Les TIC représentent aussi des instruments de connaissance. Bon nombre d'employeurs utilisent l'internet pour se renseigner sur les candidats à l'embauche. Google et Facebook, notamment, jouent ainsi le rôle d'indicateurs et révèlent au futur patron des facettes des candidats qui ne se trouvent pas sur leurs CV.

100. Il existe de nombreux cas de violations de la vie privée par les employeurs, l'un des plus célèbres, et des plus graves, étant celui de Deutsche Telekom. En 2005 et 2006, des hauts dirigeants de Deutsche Telekom (Bonn, Allemagne) avaient embauché un détective privé pour enquêter sur des allégations de fuites au sein de la société. Deutsche Telekom avait utilisé secrètement des données qui provenaient des téléphones mobiles et des ordinateurs de membres du personnel et de journalistes. A la suite de la révélation de ce scandale dans les médias en 2008, le parlement allemand et le procureur de Bonn ont commencé leur enquête. Deutsche Telekom a ensuite créé le poste de commissaire interne à la protection des données et réclamé des dommages-intérêts aux dirigeants licenciés.

101. Le Comité consultatif de la Convention no 108 analyse actuellement la nécessité de réviser la Recommandation no R (89) 2 concernant la protection des données à caractère personnel utilisées à des fins d'emploi.Un rapport préparé pour le comité consultatif par M. Giovanni Buttarelli, superviseur adjoint de la protection des données à l'Union européenne, formule des propositions pour réviser cette recommandation du Conseil de l'Europe. Il suggère qu'«il serait souhaitable de décourager plus explicitement les activités impliquant, même de manière discontinue, le traitement de données à caractère personnel visant directement et principalement à opérer une surveillance à distance (physique ou virtuelle) de l'activité professionnelle et d'autres activités personnelles. L'employeur devrait s'abstenir d'utiliser les résultats de tels traitements illicites, même si les travailleurs en ont été informés»[30].

Par les individus eux-mêmes

102. Dans bien des cas, les individus ne prennent pas la pleine mesure de la portée de leurs actions sur l'internet. Le Web 2.0 leur a donné la possibilité d'interagir, d'apporter des commentaires, de diffuser eux-mêmes du contenu, de partager en continu savoirs, photos, vidéos, informations, états d'âme, etc. Cependant, la propagation des informations sur l'internet dépasse parfois considérablement ce que l'on pourrait attendre. L'exemple des informations tirées des pages publiques de Facebook et jointes automatiquement, à l'insu de la personne concernée, par un logiciel de courrier électronique aux courriels envoyés a déjà été cité ci-dessus. La puissance des robots «ratisseurs» qui alimentent les moteurs de recherche permet de faire remonter des informations trouvées à des endroits épars, publiées à l'attention d'un

29. Voir www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf.
30. Voir www.coe.int/t/dghl/standardsetting/dataprotection/T-PD%20BUR%20(2010)%20FR%20FINAL.pdf.

public qu'on croyait restreint. Ce qui est émis dans un certain cercle (par exemple un commentaire déposé sur un forum de discussion) risque donc de réapparaître, sorti de son contexte et juxtaposé à d'autres informations.

103. Une fois l'information (texte, image, vidéo) diffusée, on ne peut plus contrôler son parcours. L'effacer du site initial n'empêchera pas qu'elle perdure dans les lieux où elle a été copiée ou téléchargée avant son effacement. Et il est illusoire de vouloir contrôler que l'usage qui est fait de l'information (notamment aux antipodes et par des inconnus) respecte la finalité de sa diffusion première.

104. Cette perte de contrôle est d'autant plus inquiétante qu'elle s'accompagne d'un «effet d'éternité». A l'inverse de la mémoire humaine, la mémoire électronique n'efface rien d'une manière involontaire. Des éléments peuvent remonter éternellement du passé tant qu'on n'a pas pris la décision, le temps et l'énergie de les supprimer (là où il est possible de les supprimer).

105. Des actes individuels malveillants peuvent aussi susciter des inquiétudes. Diffuser une information diffamatoire ou confidentielle sur Facebook, poster une vidéo intime ou humiliante sur YouTube, ou créer un faux article sur quelqu'un dans Wikipedia peut causer des dommages d'une ampleur sans précédent dans la vie «off line».

4.2. Profilage

106. Le Comité des Ministres du Conseil de l'Europe a adopté l'an dernier la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage[31]. Le profilage consiste à appliquer des algorithmes à des quantités d'informations agrégées, pour mettre au jour des corrélations entre les données et faire surgir des profils. Ces derniers sont appliqués à un individu, pour décider du traitement à lui réserver (le considérer ou non comme fraudeur fiscal, ou comme cible de marketing de tel produit, ou comme voyageur terroriste potentiel, etc.). Motivé par un intérêt économique (voir ci-dessus), sécuritaire ou autre, le profilage est facilement réalisable à partir des informations disponibles à grande échelle (traces, mots introduits dans les moteurs de recherche, etc.) et, notamment, du recours aux cookies.

107. Le profilage répond à des besoins ou intérêts légitimes de la société: analyse du risque, identification des fraudes, segmentation des marchés, ajustement de l'offre à la demande, etc. Toutefois, il peut amener à priver des individus de manière injustifiée de l'accès à certains services. L'existence de profils conduit à ce que l'information offerte est filtrée, triée, sélectionnée en fonction du destinataire. Cela vaut aujourd'hui massivement pour les informations commerciales. Sera-ce demain le cas pour toutes les informations? Le profilage risque aussi d'être un instrument de discrimination. Comment contester l'élaboration d'un profil ou son application inappropriée? La plupart du temps, l'existence des profils échappe à la connaissance des individus concernés et la compréhension de leurs critères d'élaboration échappe à ceux qui les appliquent. Enfin, l'activité de profilage suscite de graves préoccupations concernant la proportionnalité. Les quantités de données collectées et la durée de leur conservation sont dans bien des cas totalement excessives.

4.3. Rétention des données

108. Les données liées à l'utilisation de l'internet et des nouveaux moyens de communication représentent une mine de renseignements précieux pour les activités de recherche policière et de lutte contre la criminalité. Depuis les attentats du 11 septembre 2001, des textes ont été votés au niveau européen pour harmoniser les situations dans lesquelles des données relatives au contenu ou des données de trafic ou de localisation sont conservées pour être tenues à la disposition des autorités pénales. Ces données portent sur la durée, la date, les destinataires, le lieu de toutes les communications, le volume des SMS/textos et des courriels, etc.

109. Il est intéressant de voir la progression de ces textes. La Convention sur la cybercriminalité de 2001 prévoit que les Etats peuvent imposer la conservation rapide de telles données, à la demande d'une autorité, pour des données spécifiées et pour un maximum de quatre-vingt-dix jours. La Directive 2006/24/CE sur la conservation de données, quant à elle, impose aux fournisseurs de services de communication (internet, téléphone, mobiles, télécopie) la rétention des données de trafic et de localisation de tout le monde, de façon systématique et pour une durée entre six mois et deux ans. L'évaluation de cette directive est en cours.

31. https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanFrench.

5. Conclusions

5.1. Autorégulation

110. Si la technologie suscite des inquiétudes, elle offre aussi des solutions. La conception technique des outils peut veiller à la minimisation des données collectées. L'exercice des droits (d'accès, rectification, opposition) peut être facilité en prévoyant une modalité électronique en ligne. La configuration par défaut des options de diffusion des données peut être restrictive plutôt que maximaliste. Le secteur privé peut donc, par application du principe de «respect de la vie privée dès la conception» *(privacy by design)*, apporter une réponse aux préoccupations évoquées dans ce rapport. Il peut aussi adopter ou inviter les internautes à utiliser les «technologies renforçant la vie privée» (PET). La régulation du secteur privé ne se limite toutefois pas aux technologies mais devrait également couvrir les usages et pratiques en place dans ce secteur et évoquées ci-dessus.

111. Une étude sur les avantages économiques des technologies renforçant la vie privée, préparée par la société de conseil London Economics en juillet 2010 pour la Commission européenne, analyse les possibilités offertes par ces technologies pour les sociétés privées et les individus[32].

112. Une des faiblesses de l'autorégulation est qu'elle dépend de l'initiative et de la bonne volonté des personnes concernées. Il est clair qu'une plus grande sensibilisation collective met la pression sur ces personnes et peut accroître leur motivation pour des raisons liées à leur image ou celle de tout un secteur industriel. Une autre faiblesse tient au fait qu'à la différence de la législation, l'autorégulation n'est pas le fruit d'une confrontation de points de vue devant aboutir à un équilibre. Les règles établies étant la plupart du temps issues d'une seule catégorie d'acteurs, elles ne reflètent que la prise en compte des préoccupations par ces seuls acteurs et leur perception de l'équilibre socialement et économiquement admissible.

113. Les mesures d'autorégulation devraient compléter et soutenir les règles légales. Elles renforceraient très certainement leur efficacité. Elles devraient être largement encouragées mais, étant donné leurs faiblesses, ne devraient pas se substituer à l'action du législateur national ou international. Pour qu'il réussisse, un bon programme d'autorégulation devrait: apporter une valeur supplémentaire et contribuer à une mise en œuvre appropriée des principes et des règles inscrits dans le cadre légal, prenant en compte les caractéristiques spécifiques des différents secteurs; impliquer toutes les parties prenantes concernées, y compris les autorités de protection de données, dans leur phase préparatoire et d'une façon transparente; prévoir des mécanismes vigoureux de contrôle et d'exécution, qui favoriseraient la confiance des individus; mettre en place, enfin, un mécanisme pour sa révision et son amélioration régulières.

114. Cela étant, une amélioration de l'efficacité passera en outre impérativement par une plus grande sensibilisation des usagers.

5.2. Droit international

115. Les législations existantes pèchent par un manque d'efficacité et par des lacunes quant au contenu du régime de protection. Tant la Convention no 108 que la Directive de l'Union européenne sur la protection des données ont été conçues avant l'avènement de l'internet. La dimension globalisée des services d'information, le contexte virtuel et transfrontière n'ont pas pu être pris en compte lors de l'élaboration de ce régime de protection. L'opacité terriblement généralisée du système et les pernicieuses possibilités de surveillance n'ont pu être anticipées.

116. Une opération de modernisation des textes s'impose assurément, qui devrait conduire à intégrer de nouveaux principes tels celui de la minimisation des données, du renforcement de la responsabilité, du renforcement de la sécurité (incluant des obligations liées aux violations de la sécurité des données). Les droits des individus devraient être renforcés (droit d'opposition devant permettre notamment de s'opposer à une décision automatisée, droit à la suppression des données). Des obligations de transparence devraient être consacrées ou réaménagées.

117. Le respect des législations pourrait être amélioré notamment en renforçant les pouvoirs des autorités de contrôle et en instaurant un droit d'action collective en justice. Un mécanisme de contrôle des législations nationales préalablement à la ratification de la Convention no 108 pourrait aussi être mis en place.

32. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

118. La Convention no 108 est le seul ensemble de normes avancées existant dans ce secteur sous l'angle du droit international public. Il est donc nécessaire d'encourager le plus grand nombre d'Etats possible au niveau mondial à y adhérer et de commencer à rédiger un nouveau protocole à cette convention afin d'adapter les normes établies aux nouveaux défis.