Défis induits par les technologies en matière de protection de la vie privée et des données en Europe

Rapport du groupe de travail *ad hoc* «Respect de la vie privée et technologies» de l'ENISA

Juillet 2008

Élaboré par:

Mema Roussopoulos, FORTH (présidente du groupe de travail)
Laurent Beslay, CEPD
Caspar Bowden, Microsoft
Giusella Finocchiaro, Université de Bologne
Marit Hansen, ULD Kiel
Marc Langheinrich, ETH Zurich
Gwendal Le Grand, CNIL
Katerina Tsakona, FORTH

Publié sous la direction de:

Marc Langheinrich, ETH Zurich
Mema Roussopoulos, FORTH

Sommaire

1. Introduction 3

2. Synthèse des recommandations 5

3. Un récit édifiant 12

4. Disparités et défis en matière de protection de la vie privée 17

4.1 E-inclusion du respect de la vie privée 17

4.2 Outils améliorés d'aide aux utilisateurs 21

4.3 Le droit d'accès de la personne concernée aux données: mesures pour une mise en œuvre effective 24

4.4 Gérer l'identité en établissant une distinction contextuelle 28

4.5 Informations sur les incidents en matière de sécurité 32

4.6 Orientations sur les systèmes de certification 35

4.7 Outils de surveillance 37

4.8 Orientations sur les meilleures techniques disponibles 40

4.9 Mesures d'incitation et sanctions efficaces 42

4.10 Données à caractère personnel ou à caractère non personnel? 45

4.11 Protection de la vie privée et tri social 48

4.12 Respect de la vie privée, protection des données et notion d'«espace» 51

1. Introduction

Le respect de la vie privée et la protection des données à caractère personnel représentent, à ce jour, des défis majeurs pour le développement des applications et systèmes liés aux technologies de l'information et de la communication (TIC), comme l'a clairement précisé le considérant 8 du règlement (CE) n° 460/2004 du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). De nouveaux risques de traitement illégal des données à caractère personnel sont générés, entre autres, par l'émergence de l'identification par radiofréquence [*Radio Frequency Identifiers* – RFID] et par l'expansion des systèmes de télécommunication mobiles et sans fil ainsi que des applications dont la fiabilité et la sécurité de fonctionnement reposent sur des protocoles internet de bout en bout [*end-to-end*]. Les menaces potentielles découlant de la vulnérabilité à la fois technique et humaine (telles que les «pourriels» (spams) agressifs, les logiciels malveillants ou l'«hameçonnage», par exemple) commencent à être exploitées aux fins d'attaques criminelles organisées. À moins que des moyens adéquats ne soient trouvés pour garantir le respect des principes de protection des données, la prolifération attendue des réseaux de capteurs – ayant pour rôle de collecter des informations sur la vie quotidienne des individus – risque de mettre à rude épreuve notre capacité à faire appliquer ces principes.

Le groupe de travail «Respect de la vie privée et technologies» de l'ENISA a été constitué en vue d'analyser les problèmes posés par ces évolutions technologiques ainsi que les implications que celles-ci peuvent avoir sur le cadre juridique actuel de l'Union européenne. Sa tâche première consiste à proposer des actions permettant de surmonter ces difficultés. Dans le présent rapport, nous identifierons tout d'abord les principales **disparités auxquelles les technologies ont donné lieu** entre, d'une part, la réglementation relative à la protection des données et, d'autre part, la réalité de l'environnement socio-économique tel qu'il évolue peu à peu. Nous examinerons ensuite les menaces et opportunités potentielles liées aux technologies de pointe, et nous suggérerons des mesures prioritaires pour remédier aux disparités et lacunes les plus préoccupantes.

Si les principes de protection des données ont été résolument formulés en des termes dépourvus de toute connotation technologique, il n'est guère aisé de comprendre comment ces principes peuvent être, dans les faits, appliqués aux innovations qui tendent à appuyer l'objectif de Lisbonne selon lequel l'Union européenne doit devenir «l'économie de la connaissance la plus compétitive et la plus dynamique du monde». **Pour que les citoyens demeurent confiants dans les mesures qui sont prises pour protéger leurs droits fondamentaux et soient assurés que le cadre proposé par l'Union européenne est adapté à leur réalité quotidienne, ils doivent pouvoir exercer, de façon à la fois pratique et utile, leur droit au respect de la vie privée**. Il importe que ces

principes ne deviennent pas une simple abstraction juridique, ne prévoyant que des moyens de recours théoriques pour des cas exceptionnels. Une réflexion originale et des actions décisives devront sans doute être engagées pour qu'une situation aussi précaire puisse être évitée.

Dans la dernière partie du rapport, nous décrirons succinctement chacun des problèmes identifiés et nous dresserons la liste de leurs caractéristiques spécifiques; enfin, nous formulerons diverses recommandations qui nous paraissent essentielles pour combler les fossés observés. Lorsqu'il y a lieu, notre analyse prendra en considération le rôle des organismes concernés dans les secteurs public et privé, tant au niveau de l'Union européenne que de celui des États membres.

2. Synthèse des recommandations

La présente section propose une synthèse des disparités constatées ainsi que des solutions recommandées. Pour une présentation plus détaillée, nous vous invitons à consulter les descriptions individuelles de ces disparités dans le corps du document.

E-inclusion du respect de la vie privée

Parmi les problèmes cruciaux qui se posent figurent le manque de prise de conscience, voire l'incompréhension, du public concernant les problèmes liés à la protection de la vie privée, de même que l'incapacité à agir de façon appropriée. Cette situation a pour effet de créer un clivage au sein de la société, entre ceux qui parviennent à protéger leur vie privée (les «nantis») et ceux qui ne le peuvent pas (les «démunis»). Tout comme la société de l'information a dû faire face au problème de l'insertion numérique (ou «e-inclusion») des technologies de l'information et de la communication (TIC), c'est-à-dire à la question de savoir comment rendre ces TIC plus accessibles aux utilisateurs, il s'agit aujourd'hui de concentrer nos efforts sur les mesures permettant aux citoyens de mieux protéger leur vie privée et de veiller à ce que celle-ci soit davantage respectée dans le cadre des TIC. À cet égard, l'importance doit être accordée non seulement aux groupes pour lesquels les TIC représentent un véritable défi, à savoir les personnes âgées ou handicapées, mais aussi aux jeunes dont le seuil d'utilisation des TIC demeure faible.

Nous conseillons à la Commission de lancer des programmes d'«e-inclusion» permettant de toucher les citoyens grâce à la mise en place de mesures adaptées à leur situation réelle, que ce soit dans les écoles, les jardins d'enfants, les entreprises ou en tout autre lieu. Pareils programmes requièrent non seulement le développement d'outils d'aide aux débutants et de systèmes de gestion de l'identité, mais aussi de meilleurs moyens de communication (tels que des brochures sur le respect de la vie privée, des programmes d'éducation dans les écoles, etc.).

Outils d'aide aux utilisateurs

Ni les meilleures technologies ni la législation la plus pertinente ne peuvent aider les citoyens si ceux-ci sont incapables de les exploiter au mieux de leurs intérêts. À titre d'exemple, les utilisateurs finals n'ont guère recours à certaines technologies de sécurité, telles que le cryptage et l'anonymisation, en dépit de leur sophistication technique. Les responsables du traitement des données, dont le modèle de fonctionnement est tributaire de la valorisation financière des flux de données à caractère personnel, ne sont pas suffisamment incités à fournir aux personnes concernées des interfaces de contrôle ergonomiques.

Nous recommandons aux entreprises et aux organismes de recherche de consacrer des ressources au développement d'interfaces utilisateurs plus utiles et d'emploi plus aisé ainsi que de guides intelligents pour la configuration correcte de systèmes et le contrôle des données à caractère personnel. Afin d'aider les personnes concernées à prendre davantage conscience des implications que le traitement de données à caractère personnel peut engendrer, les États membres, les autorités chargées de la protection des données (DPA) et les associations de consommateurs devraient accroître leurs efforts en matière d'éducation, si possible en les adaptant aux groupes spécifiques de citoyens auxquels ils s'adressent (jeunes gens, parents, ...).

Accès en ligne des données par la personne concernée

Un des éléments les plus marquants du cadre communautaire de protection des données est le droit, solidement ancré dans la législation, qui est reconnu à toute personne concernée de découvrir ce que les organisations savent sur elle, c'est-à-dire le droit d'accès aux données à caractère personnel. Toutefois, et bien que les raisons initiales ayant motivé l'établissement de ce droit revêtent une importance et un degré d'urgence croissants, l'application de ce droit n'a pas évolué au même rythme que d'autres aspects du développement de la société de l'information, ce qui entrave son exercice approprié et efficace. Pour favoriser cette application, le souci premier doit être de garantir l'authentification correcte de la personne qui introduit la demande d'accès.

Nous recommandons à l'ENISA et au groupe de travail «Article 29» de procéder à une analyse détaillée de la politique en la matière, en vue d'offrir aux personnes concernées la possibilité d'accéder en ligne – idéalement sans aucun frais – à un maximum de données les concernant. Dans la mesure du possible, ce remaniement devrait pouvoir se faire dans le respect du cadre juridique existant. Dans ce contexte, les outils d'aide aux utilisateurs et les systèmes de gestion de l'identité peuvent jouer un rôle notable.

Gestion de l'identité

Pour garantir la responsabilisation dans le cadre des activités en ligne, les systèmes TIC actuels demandent généralement aux utilisateurs d'introduire leur véritable nom et certaines informations personnelles complémentaires, attestées par des certificats numériques. Cependant, l'introduction du nom de l'utilisateur se révèle souvent superflue. Les «*private credentials*» [justificatifs d'identité ou authentifiants] ou «*minimum disclosure certificates*» [certificats minimaux de divulgation] permettent, avec un niveau accru de protection de la vie privée, de prouver les autorisations données, tout en contrôlant les conditions qui déterminent le caractère identifiable et la responsabilisation de l'utilisateur. La possibilité de disposer de ces technologies a des implications sur l'interprétation du principe de minimisation des données et sur la signification du concept de

proportionnalité, à savoir que le traitement des données à caractère personnel ne devrait pas être excessif, mais devrait au contraire se limiter à ce qui est strictement nécessaire.

Nous recommandons aux législateurs et aux décideurs politiques, tant au niveau national qu'européen, de réexaminer les motifs de légitimité du traitement des données à caractère personnel à la lumière des technologies susmentionnées. Nous conseillons, en outre, aux parties prenantes des secteurs public et privé d'œuvrer à la mise en place des infrastructures nécessaires pour l'émission et l'interopérabilité des justificatifs d'identité, et le cas échéant – d'en faire usage dans leurs systèmes TIC.

Notification des incidents en matière de sécurité

Assurer une protection efficace de la vie privée n'est possible que si des informations sont communiquées, de façon appropriée et en temps opportun, concernant les risques que le traitement des données comporte en termes de sécurité et de protection de la vie privée, ainsi que les incidents survenus à cet égard et impliquant des données à caractère personnel.

Nous recommandons à la Commission européenne d'introduire une législation exhaustive sur la notification des violations de la sécurité. En particulier, cette législation devrait permettre non seulement aux autorités chargées de la protection des données mais aussi à chaque individu de mieux identifier ces incidents et de réagir plus adéquatement. De la sorte, les citoyens comprendront mieux comment ils peuvent être concernés par les incidents relatifs à la sécurité et à la protection de la vie privée, et ce qu'il y a lieu de faire en pareils cas. Par ailleurs, nous recommandons aux organismes de normalisation d'examiner la possibilité de travailler sur des formats et des protocoles supportant les systèmes TIC des utilisateurs pour permettre l'interprétation de ces notifications.

Certification

Les démarches entreprises pour encourager la conformité au moyen de mesures d'incitation exclusivement économiques n'ont guère eu de succès à ce jour. D'autres approches doivent, dès lors, être envisagées pour favoriser la conformité. À titre d'exemple, les États membres devraient concevoir des instruments destinés aux entreprises, afin que celles-ci puissent fournir une certification ou autocertification de leur conformité à la législation sur la protection des données, lorsqu'elles répondent à un appel d'offres public. Les États membres devraient promouvoir et régir la mise en place de systèmes de certification, en impliquant aussi les associations de consommateurs. Ils devraient ainsi offrir des avantages fiscaux aux entreprises respectueuses de la vie privée, voire envisager l'exemption des sociétés de certaines obligations de déclaration à la condition qu'elles disposent d'une certification en matière de protection de la vie privée (à l'instar de l'ordonnance suisse sur la certification

en matière de protection des données, OCPD/VDSZ[1], qui est entrée en vigueur le 1er janvier 2008). Des sanctions (et une indemnisation) efficaces devraient être prévues en cas de violation de la législation sur la protection des données (telles que des sanctions sur une base journalière ou des dommages-intérêts punitifs).

Nous conseillons à la Commission européenne d'encourager la mise en place de procédures de certification en matière de protection de la vie privée, et d'élaborer des dispositions fiscales et autres pour favoriser l'adoption de cette certification. Nous recommandons, en outre, aux organismes de normalisation de contribuer à normaliser les référentiels de certification dans ce domaine. Le cadre global de certification devra inclure, parmi ses composants majeurs, des outils de surveillance et les meilleures techniques disponibles.

Outils de surveillance

Les autorités chargées de la protection des données (DPA) rencontrent des difficultés pour inspecter et contrôler les systèmes de traitement des données à caractère personnel. De leur côté, les entreprises ne disposent pas d'outils adéquats pour procéder à des audits internes sur le respect de la vie privée. À l'heure actuelle, ni les technologies les plus avancées ni le cadre juridique n'offrent les moyens de superviser et d'inspecter aisément les opérations menées par les responsables du traitement des données. Or, il devrait être possible de mettre en place des outils normalisés de surveillance avec accès automatisé, voire avec possibilité d'accès à distance par les DPA, afin que ces dernières puissent exercer leurs pouvoirs d'inspection de façon appropriée et continue. Ces outils devraient, en outre, garantir la traçabilité irréfutable des systèmes et, partant, contribuer à améliorer les procédures d'inspection et faciliter l'analyse de toute violation de la vie privée. Enfin, pareils outils de surveillance devraient favoriser la transparence et stimuler la communication d'informations sur le traitement des données à l'utilisateur.

Nous recommandons à la Commission européenne de financer des recherches en vue de mettre au point des outils efficaces de surveillance du respect de la vie privée, permettant d'effectuer des contrôles d'une totale fiabilité. Par la suite, les responsables du traitement des données devraient systématiquement avoir recours à ces outils pour assurer une surveillance continue du respect de la vie privée et les DPA devraient aussi les utiliser pour automatiser leurs inspections.

Meilleures techniques disponibles

Pour que les systèmes de collecte et de traitement des données puissent faire l'objet de procédures d'audit et de certification à la fois efficaces et opportunes, tant les entreprises que les DPA doivent pouvoir disposer d'une palette

[1] Voir http://www.admin.ch/ch/f/rs/235_13/index.html

déterminée des meilleures techniques disponibles (MTD) en matière de sécurité et de protection de la vie privée. Une approche du type «liste de contrôle» doit être prise en compte pour l'évaluation de la conformité aux règles en matière de protection de la vie privée et l'établissement d'une certification élémentaire qui puisse servir de base pour le développement d'autres outils d'analyse et de contrôle.

Nous recommandons à la Commission de proposer un instrument juridique qui définisse la structure et les procédures requises pour la sélection de ces MTD. Cet instrument devrait prévoir la participation active de toutes les parties concernées. Les opinions communiquées par ces dernières devraient être considérées comme des lignes directrices essentielles par les autorités de contrôle et les organismes publics et privés qui mettent en œuvre les systèmes de traitement des données.

Mesures d'incitation et sanctions

Force est de constater que, dans l'ensemble, les responsables du traitement des données ne sont pas suffisamment motivés à respecter la législation sur la protection des données. La plupart des autorités de protection des données ne peuvent contrôler qu'un petit nombre de responsables, de sorte que les infractions à la législation passent souvent inaperçues. Qui plus est, les mesures économiques destinées à inciter ces mêmes responsables à observer les dispositions juridiques en vigueur se révèlent souvent insuffisantes, compte tenu de la légèreté des sanctions prévues.

Nous recommandons à la Commission européenne et aux États membres d'encourager l'établissement d'un système incitatif lié à un programme de certification et d'un mécanisme efficace de sanctions économiques, fondé sur les MTD, ainsi que d'outils valables d'audit et de surveillance.

Données à caractère personnel ou à caractère non personnel?

Malgré les efforts déployés récemment par le groupe de travail «Article 29» en vue de clarifier la notion de «donnée à caractère personnel», celle-ci est encore souvent remise en cause. Même lorsque les entreprises sont d'avis qu'aucune donnée à caractère personnel n'est impliquée, une analyse des risques de violation de la vie privée devrait être effectuée et le système devrait être conçu de manière à minimiser ces risques. Dans certains cas, des données peuvent revêtir un caractère personnel, en particulier si les moyens pouvant être raisonnablement utilisés pour identifier une personne évoluent au fur et à mesure que de nouvelles technologies apparaissent. Il s'ensuit que, même pour les données n'ayant pas vocation à devenir «personnelles», des mesures de prévention appropriées devraient être mises en œuvre afin d'éviter tout risque qu'elles ne le deviennent.

Nous recommandons, d'une part, à l'ENISA de définir des méthodes d'évaluation des incidences sur la vie privée et, d'autre part, aux entreprises de tenir compte de ces évaluations lors de l'élaboration de leur politique en matière de sécurité et de protection de la vie privée. Nous conseillons aussi aux entreprises de concevoir et mettre en place des garde-fous appropriés pour protéger adéquatement les données qu'elles détiennent, que celles-ci revêtent ou non un caractère personnel.

Tri social

Le tri social, tel que le marketing comportemental, peut porter atteinte à la vie privée des citoyens, même si les données traitées n'ont pas un caractère personnel. À l'heure actuelle, les dispositions légales en la matière sont disséminées dans différents actes juridiques et n'offrent pas, en pareils cas, une protection efficace de la vie privée.

Nous recommandons que la Commission développe et établisse un cadre juridique global pour le traitement de toutes les données concernant des individus, que celles-ci revêtent ou non un caractère personnel. En pratique, ce cadre pourrait imposer une piste de vérification intégrale du traitement et des sources de données ainsi que l'obligation de renforcer la transparence à l'égard des personnes concernées. Nous conseillons, par ailleurs, que les responsables du traitement des données instaurent des mesures organisationnelles et techniques qui garantissent aux personnes concernées la possibilité d'exercer leurs droits.

Respect de la vie privée, protection des données et notion d'«espace»

La société de l'information représente clairement un défi en termes de conservation des données personnelles des citoyens relevant de la compétence de l'Union européenne. En digitalisant le domaine personnel de même que ses limites, le concept du «territoire numérique» offre la possibilité d'introduire les notions de «territoire», de «propriété» et d'«espace» dans un environnement numérique. L'objectif visé est de fournir des outils qui permettent aux utilisateurs de gérer la proximité ou, au contraire, la distance qu'ils souhaitent avoir avec d'autres utilisateurs dans ce futur environnement à intelligence ambiante, tant sur le plan juridique que sur le plan social, comme c'est le cas actuellement dans le monde réel.

Nous recommandons au groupe de travail «Article 29» et à la Commission européenne d'étudier la possibilité d'appliquer la notion de territoire à la société de l'information et d'étendre certains principes juridiques au monde en ligne, dont le principe du refuge légal appliqué au domicile.

Travaux futurs

Certains des problèmes relevés ont trait aux risques que font peser, pour la protection de la vie privée, les nouveaux modèles commerciaux qui ciblent des consommateurs individuels à l'aide de la méthode de «profilage comportemental». Le groupe de travail fait observer que ces problèmes ont été soulevés récemment, mais non résolus, dans le cadre des enquêtes sur la concurrence menées aux États-Unis et dans l'Union européenne. Il recommande à l'ENISA de commander une nouvelle étude approfondie sur ces questions, en se focalisant particulièrement sur l'économie comportementale. En outre, le groupe souligne que, bien que le secteur commercial et certains organismes de surveillance affirment qu'il existe des mesures d'incitation de nature à atteindre un niveau satisfaisant d'autorégulation, les recherches universitaires existantes[2,3] ne font état que de très peu d'éléments étayant cette thèse. Il conviendrait peut-être de s'interroger sur la nécessité de nouveaux principes en matière de protection de la vie privée et de nouvelles structures de marché, afin de garantir le renforcement (au lieu de l'ébranlement) des mesures de protection de la vie privée par les forces concurrentielles. L'ENISA est en bonne position pour promouvoir ce type de recherche, en tant que facilitateur indépendant du réseau d'envergure européenne et des analyses de l'information, et pour veiller à ce que ses conclusions soient prises en compte dans le cadre des politiques communautaires.

Nous recommandons à l'ENISA de commanditer une étude afin de poursuivre les travaux sur la problématique de la protection de la vie privée et des technologies, et pouvoir ainsi mieux l'appréhender. Il conviendrait, notamment, de procéder à une analyse approfondie de la structure de marché des services en ligne soutenus par la publicité, en général, et de l'influence économique du profilage comportemental, en particulier. L'accent devrait être mis sur l'observation effective des principes de protection des données et sur l'autonomie de la personne concernée. L'étude devrait évaluer, de façon critique, l'efficacité potentielle de l'autorégulation et examiner également si les divergences concernant la définition de la notion de «données à caractère personnel» donnent lieu à un arbitrage réglementaire[4,5] entre les États membres.

---

[2] Voir http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

[3] Tseng, Jimmy C., *An Economic Approach towards Privacy Enforcement*, exposé présenté lors de l'atelier de travail «PRIME/ERIM Privacy for Business Workshop», Rotterdam, décembre 2004. Voir https://www.prime-project.eu/events/external/ERIM%20Privacy%20for%20Business%20Workshop/Tseng3.ppt.

[4] Reidenberg, Joel R., et Paul M. Schwartz, *Data-Protection Law and On-Line Services: Regulatory Responses*, Bruxelles, 1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf.

3. Un récit édifiant

La présente section décrit un scénario réaliste, vu par un utilisateur, qui démontre bon nombre des disparités et défis énumérés dans la section précédente et dont un exposé plus détaillé sera fourni dans la section suivante.

Sylvia a été confrontée récemment à des problèmes concernant le respect de sa vie privée. Depuis quelque temps, le portail ouvrant sur son moteur de recherche favori affiche des publicités qui, étrangement, semblent avoir un rapport avec des aspects de sa vie privée. Qui plus est, certaines de ces publicités concernent une affection au sujet de laquelle elle a fait des recherches en ligne. Sylvia est inquiète car elle pensait avoir pris la précaution de ne s'être enregistrée sur aucun des sites web qu'elle a consultés lors de sa recherche et de ne pas avoir introduit la moindre information personnelle susceptible de l'identifier. En outre, elle est déconcertée par le fait que, lorsqu'elle clique sur certaines publicités qui l'intéressent, elle reçoit une offre dont les conditions sont moins favorables que celle qui s'affiche lorsqu'elle utilise l'ordinateur d'un ami. Elle pense que cela a sans doute à voir avec les cookies *[mouchards électroniques], mais lorsqu'elle tente de comprendre le rôle joué par les différents types de* cookies *et comment les contrôler, tout cela lui paraît très confus. Toutefois, si elle supprime et déconnecte purement et simplement tous les* cookies *présents dans son logiciel de navigation, la consultation de la plupart des sites web qu'elle apprécie devient très peu commode.*

Elle sait que la législation en vigueur dans son pays en matière de protection des données lui confère le droit d'accès aux informations qu'une organisation quelconque détient à son propos. Elle est stupéfaite de constater que, lorsqu'elle examine les politiques en matière de protection de la vie privée des sites web qu'elle consulte, ceux-ci semblent prétendre que, à moins que le visiteur ne s'enregistre et ouvre une session, ils ne collectent pas la moindre information personnelle. Elle ne voit donc pas quelle démarche elle pourrait entreprendre pour exercer son droit légal à découvrir ce qui se passe.

Sylvia communique parfois son adresse électronique et son numéro de téléphone mobile sur des sites web offrant des services en ligne ainsi qu'à quelques boutiques commerçantes où elle achète divers produits. Elle remarque que, lorsqu'elle se rend dans d'autres boutiques, il n'est pas rare qu'elle reçoive beaucoup de courriels publicitaires et de messages par SMS pour des produits similaires à ceux qu'elle recherche. Elle commence à se demander si ces publicités n'ont pas un lien avec les petites étiquettes électroniques qu'elle a remarquées sur certains produits dont elle a fait l'achat. Ces publicités apparaissent aussi sur le navigateur de son téléphone mobile tandis qu'elle se

[5] Bohm, N., et Clayton, R., *Open Letter to the Information Commissioner*, Foundation for Information Policy Research, mars 2008, http://www.fipr.org/080317icoletter.html.

déplace dans la ville et elle doit se rendre sur la page internet correspondante pour demander sa désinscription, ce qui l'agace de gaspiller ainsi la largeur de bande pour laquelle elle paie. Pourtant, elle a beau répéter à maintes reprises ces demandes d'exclusion, elle continue toujours à recevoir des publicités importunes d'un nombre croissant de sociétés.

Sylvia est une militante active pour une cause politique controversée. Bien que ses activités soient légitimes, son ami Michael (qui utilise parfois son ordinateur) a été arrêté par la police alors qu'il se rendait à des manifestations et a dû répondre à de nombreuses questions lors d'une visite dans un pays étranger. Elle se rend compte que des liens semblent avoir été établis, sans qu'elle puisse expliquer comment, entre ses habitudes de navigation sur l'internet, ses déplacements dans la ville et les produits qu'elle achète. Elle se demande combien de temps ces informations sont conservées et si la législation en vigueur dans son pays autorise la police à y accéder et dans quelles conditions. Il lui arrive de lire, dans les médias, des articles concernant de nouvelles lois à cet égard, mais ils semblent toujours se contredire dans les détails, voire être délibérément confus. Alors qu'elle se rend à une autre manifestation, sa voiture est arrêtée par la police et elle est interrogée au sujet d'une peinture par pulvérisation et de certains outils qu'elle a récemment achetés (et payés en espèces) dans une quincaillerie pour faire quelques réparations chez elle. Elle doit aussi s'expliquer sur les raisons pour lesquelles elle a consulté un certain site web à caractère politique. De retour à la maison, elle remarque que les articles qu'elle a achetés portent des étiquettes d'identification par radiofréquence (RFID); en revanche, elle ne voit vraiment pas comment la police pouvait être au courant à propos du site web.

Elle téléphone au service des renseignements afin de prendre contact avec l'autorité chargée de la protection des données (DPA) dans son pays. Il s'avère que le site web en question est basé dans un autre État membre de l'Union européenne et il lui est conseillé de s'adresser à la DPA de cet État. Après avoir envoyé plusieurs messages électroniques à la DPA étrangère, elle obtient une réponse d'une personne comprenant sa langue et ayant compris ce qu'elle souhaitait faire. Cette personne lui conseille de prendre contact avec le site web. Cependant, les messages électroniques que Sylvia transmet à ce site restent lettre morte ou sont uniquement suivis d'une réponse automatisée qui n'est d'aucune utilité. Pour finir, elle décide d'écrire une lettre au siège social de la société responsable du site web, laquelle ne figure pas sur le site mais que Sylvia est parvenue à trouver dans le registre public des «responsables du traitement des données». Elle est toutefois confrontée à un problème: comme, dès le début, ce site web ne lui inspirait guère confiance, elle s'est enregistrée sur le site en utilisant un nom d'emprunt. Après plusieurs autres échanges avec la DPA et les responsables du site web, ceux-ci accèdent finalement à sa demande, en posant comme condition qu'elle leur communique, dans sa lettre, le mot de passe pour l'accès à son compte. Bien qu'elle ne comprenne pas vraiment pourquoi elle doit donner son nom et son adresse véritables

(puisqu'elle doit, de toute façon, indiquer le nom du compte et le mot de passe), elle renonce à argumenter sur ce point avec la DPA et les responsables du site web. Après avoir envoyé un mandat postal international d'un montant de quinze euros (le site web n'acceptant pas les paiements en ligne), elle reçoit, un mois plus tard, un paquet de documents reprenant les rapports imprimés de son utilisation du service de messagerie du site web, mais aucune information concernant les cookies *ou les pages qu'elle a consultées sur le site sans avoir pour autant ouvert une session. Or, c'était précisément les informations qu'elle souhaitait obtenir en tout premier lieu (et elle voulait savoir, en particulier, comment ces informations avaient pu être transférées à d'autres sites web ou aux autorités). Sylvia reprend alors contact avec la DPA qui lui explique que, d'après son interprétation de la législation nationale sur la protection des données, le site web n'est pas tenu de lui communiquer ces informations. À ce stade, Sylvia est assez déçue de voir à quel point il lui est difficile de faire valoir ses droits à la protection des données la concernant, mais aussi de constater que ces droits ne lui permettent pas, en définitive, de découvrir ce qui touche réellement à sa vie privée en ligne. Elle dispose d'une longue liste d'autres sociétés auxquelles elle pourrait écrire: les boutiques où elle a acheté des produits portant des étiquettes électroniques, les responsables des autres sites web qu'elle consulte et, bien entendu, son fournisseur de services internet (FSI) et la société de téléphonie mobile. Cependant, tout cela lui coûterait assez cher en frais d'accès et, dans la mesure où la plupart de ces sociétés risquent fort de lui répondre également qu'«elles ne savent pas qui elle est», elle s'attend à obtenir le même résultat insatisfaisant. Heureusement, Sylvia a un ami juriste spécialisé dans la protection de la vie privée, qui accepte de se charger de l'affaire. Après six mois de persévérantes enquêtes et une multitude de courriers juridiques, elle finit par repérer les éléments d'identification par radiofréquence et les* cookies *qui doivent être, selon elle, à l'origine de l'interrogatoire auquel elle a été soumise par la police alors qu'elle se rendait à la manifestation. Toutefois, les seules entreprises qui étaient en mesure de permettre à la police de reconstituer sa véritable identité ne lui communiqueront pas davantage d'informations. Une société lui fournit néanmoins un renseignement précieux, en attirant son attention sur une disposition de la loi sur la protection des données qui précise que les entreprises en question ne sont pas tenues de fournir des informations à la personne concernée si cette dernière est considérée comme «suspecte».*

Sylvia a le sentiment d'avoir totalement perdu le contrôle de sa vie privée et elle est même inquiète à l'idée qu'après tous les efforts juridiques entrepris pour faire valoir ses droits, elle puisse être assimilée à un «fauteur de troubles» et être inscrite sur des listes, ce qui pourrait lui occasionner encore plus de tracas à l'avenir, voire lui causer des difficultés en ce qui concerne son travail, son assurance-maladie et sa cote de solvabilité. Elle décide d'abandonner ses activités politiques, de retirer toutes les étiquettes des produits en sa possession, de se procurer un nouvel ordinateur, de changer de fournisseur de services internet, de fermer tous ses comptes en ligne et d'utiliser un téléphone mobile

prépayé. Elle n'est pas sûre pour autant que sa trace ne sera plus suivie. Elle fait part à ses amis de ses expériences surréalistes avec la bureaucratie en matière de protection de la vie privée, mais ils ne la croient pas vraiment et pensent qu'elle devient un peu loufoque. Après tout, ils savent que l'Europe dispose de la législation la plus rigoureuse en matière de protection de la vie privée et ils ne pensent pas que ce soit un problème dont la plupart des citoyens, les médias ou les politiciens devraient se préoccuper.

Toutefois, Sylvia découvre l'existence d'un nouveau progiciel qui fonctionne avec plusieurs sites web très prisés et jouissant d'une bonne réputation quant au respect de la vie privée. Ce progiciel lui permet de télécharger sur son ordinateur l'inventaire complet des informations relatives aux interactions qu'elle a eues avec un site web. Elle est surprise par l'ampleur des informations détaillées qui sont stockées au sujet de ses habitudes de navigation; elle remarque, en outre, que certaines de ces informations ont été divulguées – via des cookies *– à d'autres sociétés à des fins publicitaires. Elle choisit un fournisseur de services internet qui participe à ce programme, ce qui lui permet de découvrir quelle «adresse IP» elle utilisait à tout moment. Grâce à cette information, elle peut aller sur d'autres sites et trouver automatiquement les données qu'ils détiennent concernant les pages qu'elle a consultées sur ces sites; néanmoins, cette possibilité n'est offerte que dans certains États membres de l'Union européenne qui reconnaissent le «caractère personnel» de ces données. Le progiciel est même doté d'une fonction d'analyse qui lui permet de comparer, pour les différents sites web, la durée de conservation des données relatives à son comportement en ligne et de déterminer s'ils se conforment ou non à la politique sur la protection de la vie privée. Elle constate, néanmoins, que la politique affichée par la plupart des sites est trop vague pour que le progiciel puisse réellement exécuter cette fonction. De plus, le progiciel ne travaille qu'avec un nombre assez limité de sites web et certains des sites qu'elle considère comme les plus utiles pour elle ne participent pas au service de téléchargement. Curieusement, quelques-uns des sites les plus innovateurs aux États-Unis commencent à proposer un service de téléchargement des «*données d'attention*» [données relatives aux centres d'intérêt du visiteur d'un site]. Toutefois, Sylvia a désormais appris à être très prudente et à regarder ce qui est indiqué en très petits caractères car elle se rend compte que toute autre personne qui se procurerait ces données pourrait en tirer des conclusions quant à certaines de ses pensées les plus intimes.*

Son avocat a aussi de bonnes nouvelles à lui annoncer: après plus de deux ans, Sylvia a enfin eu gain de cause devant un «tribunal compétent en matière d'affaires relatives à des données», dont l'existence est assez confidentielle, et la police a reconnu que Sylvia n'aurait jamais dû être considérée comme une «personne suspecte». Cette dernière découvre finalement que les entreprises avec lesquelles elle a été en contact ont, à de nombreuses reprises, divulgué à la police des informations sur sa «vie électronique». La mauvaise nouvelle tient au fait que toutes ces opérations de divulgation de données ont été effectuées selon

des procédures correctes (elles étaient considérées, à l'époque, comme «proportionnées» au regard des informations disponibles et des circonstances). Sylvia ne peut, par conséquent, prétendre à aucune indemnisation de la part de la police ou de l'une quelconque des entreprises en cause pour tous les désagréments et tracas bureaucratiques (c'est le moins qu'on puisse dire) auxquels elle a été confrontée. Apparemment, tous les «officiels» considèrent que tout a été fait dans les règles de l'art.

Sylvia se demande aujourd'hui pourquoi prendre le risque de s'engager dans une activité politique en vue de faire bouger les choses sur le plan social, dès lors que les conséquences peuvent être aussi perturbantes. Elle sait que la démocratie n'est nullement parfaite et que la justice peut fonctionner parfois de façon désordonnée, mais la vie électronique moderne a, selon elle, un effet dissuasif sur l'engagement citoyen et a donné lieu à un État de surveillance qui l'effraie. L'un dans l'autre, elle en a assez de la politique (et des activités en ligne), mais elle se demande de quel genre de démocratie ses enfants vont hériter si tout un chacun pense de même et cesse aussi toute action politique. Elle réalise qu'elle n'aurait jamais pu comprendre ce qui lui est arrivé sans l'aide de son ami juriste (dont elle n'aurait jamais pu payer les honoraires). Certes, le progiciel d'accès et de gestion de ses propres données à caractère personnel lui aurait été très utile si elle l'avait trouvé plus tôt, puisqu'il lui aurait permis d'évaluer dans quelle mesure son comportement en ligne l'exposait à des risques en termes de protection de sa vie privée. Cependant, elle vient de lire que la société informatique qui fabriquait ce progiciel a arrêté sa production. Il semble que trop peu de gens soient suffisamment soucieux de protéger à tout moment leur vie privée pour que le progiciel en question soit rentable. De toute façon, la majeure partie des sites web qu'elle appréciait le plus n'étaient pas vraiment intéressés à s'inscrire dans cette démarche.

Liens

Des scénarios beaucoup plus détaillés sont présentés au chapitre «*Dark Scenarios*» du document intitulé *Safeguards in a World of Ambient Intelligence (SWAMI)*, accessible à l'adresse suivante: http://is.jrc.es/pages/TFS/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf.

4. Disparités et défis en matière de protection de la vie privée

Le chapitre suivant expose les douze disparités principales que le groupe de travail a constatées entre la réglementation relative à la protection des données et la réalité de l'environnement socio-économique tel qu'il évolue. Chaque section débute par une description de la disparité observée, puis établit la liste des défis à relever en matière de recherche et développement technique (R&D), d'évolution juridique et de communication.

4.1 E-inclusion du respect de la vie privée

Un des problèmes majeurs qui se posent est le manque de prise de conscience, voire l'incompréhension du public concernant les problèmes liés à la protection de la vie privée ainsi que le manque de capacité à agir de façon appropriée.

Disparités spécifiques

Les citoyens n'ont pas conscience des problèmes liés au respect de leur vie privée ou sont incapables de la protéger dans le paysage actuel des TIC.

La plupart des gens ne sont absolument pas conscients des problèmes majeurs, en termes de protection de la vie privée, qui sont liés à l'utilisation des nouvelles techniques de collecte de données, aux réseaux sociaux, à l'omniprésence de la technologie et à d'autres facteurs similaires. Si certains se sentent mal à l'aise par rapport à certaines formes de traitement des données, ils n'appréhendent pas pour autant les conséquences possibles de leurs actions sur leur propre vie privée. D'autres encore ont conscience de ces problèmes, mais ne savent pas que faire pour sauvegarder leur vie privée. Les individus soucieux de se protéger à cet égard refusent souvent de prendre part au monde numérique et ne peuvent, dès lors, pas profiter des avantages de la société de l'information. Ceux, par contre, qui veulent en bénéficier doivent renoncer à la protection de leur vie privée, estimant n'avoir nullement le choix dans ce domaine.

Les procédures de recours sont longues et parfois inefficaces.

Parmi les utilisateurs qui savent comment préserver leur sphère privée, certains estiment trop coûteuses ou trop contraignantes les mesures qui devraient être prises pour y parvenir. Il en est de même dans les cas de violation du droit au respect de la vie privée: les procédures de recours sont généralement très longues et il n'est pas rare que les effets de l'atteinte à la vie privée ne puissent, de toute façon, pas être annulés.

Le manque de prise de conscience, de compréhension et de capacité à agir adéquatement peut créer un clivage au sein de la société, entre ceux qui parviennent à protéger leur vie privée (les «nantis») et ceux qui ne le peuvent pas (les «démunis»).

La facilité d'utilisation des outils de protection de la vie privée n'est pas un critère suffisant.

La société de l'information doit faire face au problème de l'insertion numérique ou «e-inclusion» concernant les technologies de l'information et de la communication (TIC), autrement dit à la question de savoir comment rendre ces TIC plus accessibles aux utilisateurs. Dans la mesure où les incidences sur la vie privée résultent souvent des actes posés par les utilisateurs, il sera d'autant plus urgent de relever les défis inhérents à l'«e-inclusion» si la finalité visée est de protéger la vie privée des utilisateurs dans le cadre des TIC (dont celle des personnes âgées ou handicapées). Lors de la conception d'outils destinés à protéger la vie privée, la facilité d'utilisation constitue un critère important qui n'est pourtant pas pris en compte de manière satisfaisante.

L'insertion des jeunes est indispensable.

Les jeunes – c'est-à-dire les enfants et les adolescents – sont un des groupes spécifiques de personnes qui illustrent le mieux la nécessité d'intégrer, dans le monde numérique, la notion de respect de la vie privée. Les jeunes se caractérisent, en effet, par un faible seuil d'utilisation des TIC. Néanmoins, ce sont aussi ceux qui, dans de nombreux cas, se laissent le plus aisément tentés par les services proposant des jeux ou des applications ludiques et qui divulguent ainsi des données les concernant, voire concernant leurs parents et amis.

Solutions proposées

Pour sensibiliser le grand public aux problèmes liés au respect de la vie privée, il convient d'adopter des approches différentes selon les différents groupes de personnes ciblés: les enfants, par exemple, ne peuvent pas être abordés de la même façon que les personnes âgées. Des manuels scolaires dépourvus d'humour et rédigés dans un style trop didactique ne constituent nullement un message porteur pour sensibiliser les jeunes à la nécessité de protéger leur vie privée. Il importe, au contraire, de toucher les citoyens en prenant des exemples inspirés de leur situation réelle, c'est-à-dire de ce qu'ils vivent dans les écoles, les crèches et écoles maternelles, les entreprises ou en tout autre lieu.

Défis en matière de R&D

Intégration des besoins afférents à l'éthique et au respect de la vie privée dans les TIC.

Lors de l'élaboration d'un quelconque système TIC pouvant être lié au traitement de données à caractère personnel, les besoins en matière d'éthique et de respect de la vie privée doivent être pris en considération dès le début. Au lieu de court-circuiter des pans entiers de la population, les systèmes TIC devraient permettre aux personnes concernées de protéger leur vie privée et d'exercer leurs droits à la protection des données. S'agissant de l'insertion fondée sur l'âge, des travaux ont déjà été entrepris dans le cadre du projet SENIOR[6] qui vise à fournir une appréciation systématique des problèmes inhérents aux TIC et au vieillissement, sur le plan social et en termes d'éthique et de respect de la vie privée, en privilégiant le dialogue comme principal instrument d'évaluation.

[6] http://seniorproject.eu/

Nécessité de disposer d'outils d'aide aux utilisateurs.

La mise au point d'outils d'aide aux utilisateurs, tels que les «*privacy wizards*» [guides intelligents permettant de gérer une politique de confidentialité], pourrait contribuer à mieux éduquer les utilisateurs, en particulier s'ils sont offerts gratuitement par les autorités nationales pour soutenir les citoyens dans leur démarche. À titre d'exemple, un module d'extension du navigateur capable de gérer la confidentialité des données pourrait avertir l'utilisateur des implications découlant de l'introduction d'informations personnelles sur un site web (comme le nom de jeune fille d'une mère, le numéro d'identification, etc.). Pareils outils pourraient aussi être utilisés pour définir des paramètres par défaut de protection de la vie privée, lors de la configuration de logiciels d'accès à l'internet ou de systèmes de gestion de l'identité. L'intégration de ce genre d'outil «assistant» directement dans les systèmes TIC standard permettrait de faire connaître automatiquement aux utilisateurs les effets de leurs actes en ligne sur leur propre vie privée.

Défis juridiques

Tant la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel que la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) imposent la fourniture d'informations spécifiques aux personnes concernées. Il importe que ces informations ne soient pas formulées dans un jargon juridique abscons, mais puissent, au contraire, être comprises par tous. Eu égard aux services en ligne, le groupe de travail «Article 29» a publié des avis sur l'introduction de ces demandes légales (voir, notamment, les avis WP43 et WP100). L'avis WP147 décrit, en outre, les exigences à respecter en matière d'information des enfants sur les questions de protection des données les concernant.

Nécessité d'harmoniser et de faire appliquer la législation.

Force est de constater, malheureusement, que ces recommandations ne sont guère respectées à l'heure actuelle et que même les informations de base font parfois défaut. Il convient, dès lors, de décrire de façon plus formelle et précise les dispositions contraignantes en matière d'information des personnes concernées, en veillant à les harmoniser au mieux à l'échelon européen. De plus, les discussions à cet égard devraient mettre en exergue les pratiques et moyens considérés comme idéaux pour la communication d'informations aux personnes concernées et la fourniture de données complémentaires. Le processus d'information et de sensibilisation des personnes concernées devrait, par ailleurs, faire l'objet d'évaluations dans le cadre de programmes de certification relatifs à la protection de la vie privée.

Défis en matière de communication

Nécessité d'éduquer et de former les citoyens.

Nous nous devons de diffuser régulièrement des documentaires proposant une description visuelle des dangers spécifiques que la population encourt. De même, les risques potentiels que la surveillance permanente fait peser sur les

individus pourraient être illustrés dans des brochures ou à l'aide de documents audio-visuels (tels que ceux produits dans le cadre de «*YOU decide*», par exemple), afin que les citoyens sachent où ils sont contrôlés. Il serait ainsi utile de leur proposer des simulations montrant quelles peuvent être les conséquences de la divulgation de leurs données à caractère personnel dans différents contextes. De la sorte, les citoyens pourraient mieux appréhender les risques à long terme inhérents à de nombreux types de données à caractère personnel et, en particulier, à celles considérées comme «plus sensibles» qui ont trait à la personnalité de l'utilisateur. Dans les écoles, des jeux de rôle peuvent contribuer à sensibiliser les élèves à la nécessité de protéger leur vie privée, notamment en leur faisant prendre conscience des répercussions que des données diffusées sur des réseaux sociaux peuvent avoir, des années plus tard, sur des entretiens d'embauche[7].

L'éducation dispensée au quotidien dans la famille joue aussi un rôle primordial. Diverses orientations en matière de protection de la vie privée dans le monde «non numérique» ont déjà été définies: celles-ci expliquent, par exemple, aux parents comment imprimer certains messages dans l'esprit de leurs enfants, dont l'importance de dire «non» en cas d'atteinte à leur intimité corporelle ou de ne pas suivre des personnes inconnues. Il importe, en outre, de donner aux parents les moyens d'apprendre à leurs enfants à se protéger dans le monde des TIC. Cet enseignement peut également se faire dans l'autre sens, c'est-à-dire que les enfants peuvent expliquer à leurs parents ou grands-parents les incidences des TIC sur leur vie privée et leur apprendre à utiliser des outils de protection appropriés.

Les enseignants, les familles, les médias et les organismes publics devraient tous être impliqués dans le processus d'éducation et de formation – probablement tout au long de la vie – de tous les citoyens. Ce processus devrait couvrir les aspects relatifs à l'interprétation des informations pertinentes en matière de protection de la vie privée (ex.: politiques ou labels de protection de la vie privée) et à la gestion des risques existants à cet égard.

Liens

Groupe de travail «Article 29»: recommandation 2/2001 concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne, 5020/01/FR/Final, WP 43, adoptée le 17 mai 2001, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43fr.pdf.

Groupe de travail «Article 29»: avis 10/2004 sur «Dispositions davantage harmonisées en matière d'informations», version du 25 novembre 2004,

[7] Pareils jeux de rôle ont été organisés dans plusieurs écoles le 28 janvier 2008, à l'occasion de la troisième journée européenne de la protection des données. Voir le site suivant: http://www.coe.int/t/f/affaires_juridiques/coop%C3%A9ration_juridique/protection_des_donn%C3%A9es/Default_DP_Day_fr.asp

11987/04/FR, WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_fr.pdf.

Groupe de travail «Article 29»: document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (principes généraux et cas particuliers des écoles), 00483/08/FR, WP 147, adopté le 18 février 2008, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_fr.pdf.

The Data Inspectorate, en collaboration avec la direction norvégienne de l'éducation et de la formation et le conseil norvégien des technologies: *YOU decide ... Thoughts and facts about protecting your personal data*, janvier 2007, http://www.dubestemmer.no/pdf/english-brochure.pdf.

SENIOR – Social Ethical and Privacy Needs in ICT for Older People, 7e PC, projet 2008-2009, http://seniorproject.eu/

4.2 Outils améliorés d'aide aux utilisateurs

Les outils d'aide aux utilisateurs assistent ces derniers lors des opérations d'inspection, de contrôle et de communication de leurs données et préférences.

Idéalement, toutes les personnes concernées devraient pouvoir bénéficier d'une protection omniprésente de leurs données à caractère personnel, autrement dit d'un ensemble approprié de paramètres de confidentialité par défaut, à configuration zéro et gestion zéro, qui leur permettrait de divulguer librement leurs données tout en leur garantissant le niveau de protection souhaité. Cependant, il y a fort à parier que préserver sa vie privée et sa sécurité requerra toujours des efforts de la part de chaque individu. Les mesures de protection de la vie privée et de sécurité représentent, en effet, des constructions complexes qui dépendent fortement de la situation personnelle de l'individu et du contexte particulier dans lequel les données sont échangées ou divulguées. Les outils d'aide aux utilisateurs peuvent faciliter leur tâche, en leur offrant des moyens d'inspection, de contrôle et de communication qui leur permettront de rester maîtres de leur vie privée.

Disparités spécifiques

Les outils actuels sont dispersés et incomplets.

Le monde numérique actuel ne propose aucune «suite» complète pour la protection de la vie privée des utilisateurs finals, qui puisse les aider à gérer tous les aspects inhérents à cette protection. En règle générale, les outils existants sont très épars et permettent uniquement de résoudre des problèmes très spécifiques.

Leur utilisation requiert des efforts considérables de la part des consommateurs.

De plus, la plupart des technologies axées sur la protection de la vie privée font aujourd'hui peser une lourde charge sur les épaules de la personne concernée, dans la mesure où elles supposent que cette dernière gère ses données d'identification, esquive les demandes relatives à sa localisation et veille à anonymiser le trafic internet et ce, non seulement lorsqu'elle se trouve devant son ordinateur mais aussi à tout moment de la journée, y compris dans des

situations telles que des apparitions publiques, des événements commerciaux et des rencontres privées.

Si l'on se contente d'un modèle fondé sur des avis et des choix à opérer par l'utilisateur, il est à craindre que la plupart des gens ne prennent même pas la peine d'y prêter attention, faisant ainsi du respect de la vie privée un concept élitiste réservé à une poignée de fondamentalistes en la matière. Même les personnes désireuses d'investir des ressources dans la protection de leur vie privée risquent de se faire piéger et de révéler davantage d'informations qu'elles ne le voulaient ou, tout simplement, d'être dépassées par la complexité des systèmes de traitement des données.

Si aucun contrôle n'était prévu, il est à craindre que beaucoup ne se préoccuperaient pas de préserver leur vie privée.

Solutions proposées

L'assistance aux utilisateurs pourrait se traduire par des outils technologiques mieux intégrés et plus faciles à utiliser, proposés aux parties concernées ou mis à disposition dans des situations exceptionnelles, c'est-à-dire lorsqu'une personne souhaite connaître des informations détaillées sur une saisie de données déterminée. L'assistance pourrait aussi prendre la forme d'une stratégie plus élaborée d'éducation des citoyens, visant à leur apprendre à contrôler et à gérer correctement leur vie privée.

Défis en matière de R&D

S'agissant des outils d'aide aux utilisateurs, le critère de la facilité d'emploi revêt une importance primordiale car la personne concernée ne tentera pas d'y avoir accès si ceux-ci se révèlent trop compliqués et/ou coûteux (que ce soit sur le plan temporel ou pécuniaire). Ces outils pourraient être dotés d'une fonction de «*data tracking*» [localisation et suivi des données], de manière à permettre aux utilisateurs de contrôler les flux de leurs données à caractère personnel, autrement dit de savoir quand, à qui et à quelle fin leurs données sont divulguées. Les concepteurs de systèmes devraient être spécifiquement formés pour élaborer et mettre au point des outils selon des directives de conceptualisation «exploitable» et de mise en œuvre de systèmes TIC respectueux de la vie privée. Afin de garantir une traduction correcte des dispositions réglementaires et du langage juridique dans les interfaces utilisateurs, les autorités chargées de la protection des données doivent aussi être impliquées.

Promouvoir la facilité d'utilisation des outils d'aide aux utilisateurs.

Certaines normes techniques, dont les protocoles de communication RFID, pourraient aussi inclure des références complémentaires à la législation applicable, à l'identité du collecteur de données ou à l'usage prévu et au temps de rétention des données.

Inclure des informations juridiques dans les protocoles techniques.

Défis juridiques

Utiliser des pictogrammes normalisés pour faciliter la compréhension des aspects juridiques.

En vue de rendre les politiques en matière de protection de la vie privée plus accessibles et aisées à comprendre, différents pictogrammes ont été proposés; ceux-ci illustrent le contenu de la politique en question et évitent ainsi aux utilisateurs de devoir étudier un jargon juridique souvent abscons. La normalisation de ces icônes simplifierait la compréhension des avis, de même que les choix à opérer. Toutefois, les propositions avancées à ce jour ne se focalisent pas encore sur la législation européenne relative à la protection des données.

Défis en matière de communication

Encourager activement les États et les DPA à prendre des initiatives en matière d'éducation des utilisateurs.

La mise au point d'outils d'aide aux utilisateurs pourrait et devrait être appuyée par les États. S'agissant, notamment, des domaines de l'administration et de la participation en ligne, où les États demandent à leurs citoyens de s'impliquer directement dans le traitement de leurs données, les autorités publiques nationales devraient proposer des outils exemplaires en matière de sécurité et de protection de la vie privée, et apprendre à leurs citoyens à les utiliser. Les DPA pourraient, quant à elles, bénéficier d'un équipement adéquat et avoir pour mission de soutenir les utilisateurs en les éduquant, en leur fournissant – dans la mesure du possible – des fichiers de configuration ou des guides intelligents téléchargeables pour préserver leur vie privée, en leur donnant des instructions pour se protéger au moyen de paramètres spécifiques ou en offrant un service général d'assistance. Les avatars pourraient constituer une option intéressante, en ce sens qu'ils aident les utilisateurs à comprendre et à gérer leur «personnalité en ligne» et les «identités partielles», à l'aide de métaphores très simples. Cette proposition est étroitement liée aux disparités et défis concernant l'insertion numérique du respect de la vie privée, les demandes d'accès en ligne des personnes concernées et la notification des incidents en matière de sécurité.

Liens

Des séries exemplatives d'icônes de protection de la vie privée ont été proposées, notamment, par Mary Rundle[8] et Matthias Mehldau[9].

Le projet PRIME a examiné les exigences requises pour la conception d'interfaces utilisateurs intégrées à des outils de protection de la vie privée[10].

[8] Voir http://identityproject.lse.ac.uk/mary.pdf.
[9] Voir http://asset.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf.
[10] Voir https://www.prime-project.eu/prime_products/reports/.

4.3 Le droit d'accès de la personne concernée aux données: mesures pour une mise en œuvre effective

Tout individu jouit d'un droit d'accès aux données le concernant et de rectification de ces données.

L'article 12 de la directive 95/46/CE relative à la protection des données garantit à toute personne concernée un droit d'accès aux données, c'est-à-dire le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées. Ce même article 12 confère, en outre, à toute personne concernée le droit d'obtenir du responsable du traitement, selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive 95/46/CE, notamment en raison du caractère incomplet ou inexact des données.

Les raisons pour lesquelles le droit d'accès a été initialement établi se révèlent toujours plus cruciales et impératives. Ce droit n'est pas simplement un «garde-fou» destiné à faciliter les procédures de recours dans certains cas particuliers; il devrait aussi fonctionner comme un mécanisme de transparence socio-politique de base, visant à avertir les décideurs politiques lorsque le respect de la vie privée est systématiquement menacé dans l'un ou l'autre secteur. Au cours de ces cinq dernières années, deux enquêtes Eurobaromètre ont confirmé que les personnes concernées ne sont guère sensibilisées au droit dont elles disposent en matière d'accès aux données à caractère personnel et ne s'en prévalent guère. Ce désintéressement s'explique aisément par le fait que, pour obtenir toutes les informations auxquelles une personne concernée a droit, quand elle en a besoin et sous une forme qui lui soit utile, la démarche à suivre se révèle à la fois frustrante, longue et pénible.

Disparités spécifiques

L'accès en ligne rend plus aisé l'exercice des droits au respect de la vie privée.

Le droit d'accès de la personne concernée aux données fait figure de «parent pauvre» au sein des droits de l'homme. La rhétorique de la promotion de la société de l'information va de pair avec les demandes d'efficience économique, d'innovation et de commodité pour les citoyens. Toutefois, si les personnes concernées veulent découvrir les données qui sont détenues à leur sujet et comprendre comment les conclusions qui en sont tirées influent sur la façon dont elles sont traitées, elles doivent se livrer à une véritable course d'obstacles, de nature formaliste, qui semble tout droit sortie de l'imagination de Dickens ou de Kafka. Force est de constater le manque de moyens offerts aux individus pour leur permettre d'exercer aisément leurs droits au respect de la vie privée, notamment via les fonctions d'accès en ligne qui pourraient réduire considérablement le seuil pour les personnes concernées. Cependant, même dans

le cas des services en ligne, les utilisateurs ne peuvent généralement pas accéder en ligne à toutes leurs données à caractère personnel, dont celles stockées dans des fichiers-journaux ou en cours de traitement par des systèmes de profilage, d'évaluation par score et d'exploration de données.

Pour favoriser l'application du droit d'accès, le souci premier doit être de garantir l'authentification correcte de la personne qui introduit la demande d'accès. Si le processus d'authentification est entaché d'erreurs, cela peut donner lieu à la plus terrible faille qui soit en matière de protection de la vie privée, à savoir des demandes d'accès «pré-formulées». Idéalement, l'outil d'authentification des personnes demandant l'accès à des données devrait se trouver à portée de main; celui-ci pourrait prendre la forme d'un système de gestion de l'identité «centrée sur l'utilisateur», permettant à la personne concernée de gérer les relations en ligne avec plusieurs responsables du traitement des données n'ayant pas de lien entre eux, et permettant à chacune des parties de procéder à une authentification mutuelle approfondie.

Il convient de déplorer, en outre, le manque de procédures d'accès à des données «pseudonymes», lesquelles revêtent pourtant une importance particulière dans le monde en ligne, compte tenu du grand nombre d'identificateurs qu'un utilisateur peut avoir.

L'accès en ligne devrait être accordé selon le principe de la minimisation des données.

Solutions proposées

Les personnes concernées doivent se sentir mieux soutenues dans l'exercice de leurs droits au respect de leur vie privée lors de leurs activités en ligne. Dans toute la mesure du possible, les responsables du traitement des données devraient garantir aux personnes concernées l'accès à leurs données en ligne.

Défis en matière de R&D

Pour que toute personne concernée puisse aisément exercer ses droits au respect de sa vie privée, il importe de concevoir des interfaces utilisateurs parfaitement compréhensibles. Les responsables du traitement des données ne doivent pas restreindre l'accès des personnes concernées aux données figurant dans le fichier central client. Généralement, l'accès à la lecture en ligne des données ne pose pas de problème, pour autant que l'utilisateur ait été authentifié et que les données à caractère personnel demandées puissent être affichées séparément des autres informations protégées. Néanmoins, il n'est pas toujours aussi facile de procéder à la rectification ou à l'effacement en ligne de données, en particulier lorsque d'autres objectifs conflictuels empêchent le déroulement de cette opération. Par exemple, les utilisateurs ne devraient pas pouvoir modifier les pistes de vérification ou les preuves numériques. Des recherches doivent être menées en vue de:

L'accès en ligne fourni par le responsable du traitement doit être conçu dans une optique de facilité d'utilisation.

- structurer les systèmes dont les responsables du traitement des données disposent, afin de minimiser l'effet des exemptions (ex.: donnée

concernant exclusivement la personne concernée et ne déclenchant pas d'autres exemptions);

- proposer des options stratégiques pour imposer progressivement des obligations aux responsables du traitement des données qui entretiennent des relations en ligne avec les personnes concernées au sujet de leur identité, de manière à s'assurer qu'elles sont capables de remplir les demandes d'accès en ligne, en toute sécurité et dans toute la mesure du possible.

Des outils aidant les utilisateurs à exercer leurs droits au respect de leur vie privée.

En outre, les utilisateurs peuvent être dotés d'outils capables de les aider à transmettre des demandes au responsable du traitement ou, le cas échéant, de déposer une plainte auprès d'une autorité de surveillance. Ces outils peuvent tirer parti des fonctionnalités liées à la gestion de l'identité contrôlée par l'utilisateur et aux procédés de lecture par machine des politiques de protection de la vie privée. L'accent doit être mis sur les points suivants:

- levée des barrières à l'exercice des droits d'accès aux données, qui ne sont pas appropriées à la situation d'accès en ligne;
- adoption des mesures de «*meta-privacy*» [protection de la vie privée au niveau des métadonnées] nécessaires pour protéger les individus de toute interférence, surveillance ou discrimination résultant de l'exercice de leurs droits d'accès;
- procédures garantissant l'exercice du droit d'accès contre des responsables «indirects» du traitement des données (c'est-à-dire ceux qui détiennent des données qui ne peuvent être attribuées à une personne qu'au moyen d'un identificateur caché sous un pseudonyme).

Mécanismes de minimisation des données pour l'accès à ses propres données.

Pour qu'une personne puisse exercer son droit d'accès à des données à caractère personnel, elle doit fournir des éléments prouvant son identité, de sorte que les données demandées ne soient pas divulguées à une personne non autorisée. Si un utilisateur a communiqué des données sous le couvert d'un pseudonyme, la preuve devra être apportée que la personne qui a introduit la demande d'accès est réellement celle qui s'est enregistrée sous ce pseudonyme. Il importe, à cette fin, de disposer de mécanismes d'authentification adéquats, fonctionnant selon le principe de la «minimisation des données» et offrant les garanties suivantes:

- une authentification mutuelle approfondie de la personne concernée et du responsable du traitement des données, grâce à un système de gestion de l'identité «centrée sur l'utilisateur», permettant de soumettre et de compléter des demandes d'accès en ligne;
- un niveau supérieur d'authentification pour la personne concernée, de sorte que l'activation d'un mécanisme d'accès en ligne avec un responsable du traitement particulier puisse être autorisée sans équivoque possible.

Défis juridiques

Imposer juridiquement la fourniture d'un accès en ligne.

Pour les services traitant des données à caractère personnel sur l'internet ou d'autres informations en ligne, il devrait être imposé légalement de fournir, dans la mesure du possible, un accès aux données ou d'autres moyens en ligne permettant d'exercer ses droits au respect de la vie privée.

Exiger l'utilisation de pseudonymes appropriés pour l'accès selon le principe de la minimisation des données.

Il convient, en outre, de se demander s'il est ou non opportun d'accepter des pseudonymes dont la personne concernée ne peut pas prouver qu'elle en est détentrice en introduisant un minimum d'informations personnelles et, à tout le moins, en n'étant pas tenue de révéler son identité civile (principe de la minimisation des données), dès lors que l'usage de tels pseudonymes empêche ensuite la personne concernée d'exercer ses droits au respect de sa vie privée. Il pourrait aussi être nécessaire d'envisager:

- des propositions de garde-fous juridiques supplémentaires contre les risques d'accès coercitif aux données;
- un cadre pour les organismes de surveillance, qui leur permette d'apprécier le bien-fondé des mesures de sécurité protégeant les mécanismes et procédures d'accès en ligne.

Défis en matière de communication

Informer les citoyens sur leurs droits au respect de la vie privée.

Tant les citoyens que les responsables du traitement des données doivent être informés sur les droits au respect de la vie privée des personnes concernées et sur les possibilités qui leur sont offertes pour pouvoir les exercer.

Liens

Le projet PRIME – *Privacy and Identity Management for Europe*[11] – du sixième programme-cadre (6e PC) a proposé divers moyens d'intégrer, dans les systèmes de gestion de l'identité contrôlée par l'utilisateur, un accès en ligne pour les personnes concernées.

Dans certains États, les citoyens disposent d'un accès en ligne aux données les concernant dans les fichiers du registre national, y compris le fichier-journal contenant la clé d'accès à leurs données (ex.: «mijndossier/mondossier» en Belgique et «minside» en Norvège).

Enquêtes Eurobaromètre sur la protection des données:

- *La protection des données*, Eurobaromètre spécial n° 196 – Vague 60.0 — European Opinion Research Group EEIG, sondage commandité par la direction générale du marché intérieur et des services (unité E4, Médias et protection des données), décembre 2003, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_protection_donnees.pdf;

[11] https://www.prime-project.eu/

- *La protection des données au sein de l'Union européenne: les perceptions des citoyens*, rapport analytique, Flash Eurobaromètre n° 225, sondage effectué par Gallup Organization Hungary à la demande de la direction générale de la justice, de la liberté et de la sécurité, février 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

4.4 Gérer l'identité en établissant une distinction contextuelle

Le caractère contraignant de la finalité des données constitue un principe juridique important en Europe.

Il est notoire que l'accumulation de données à caractère personnel peut entraîner de graves atteintes au respect de la vie privée. Le principe énoncé dans la directive 95/46/CE sur la protection des données, qui confère un caractère contraignant aux finalités des données, vise à limiter la saisie et l'utilisation des données aux seules finalités préalablement déterminées: «Les États membres prévoient que les données à caractère personnel doivent être: […] b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. […] c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement […]» (article 6, paragraphe 1, de la directive 95/46/CE sur la protection des données).

L'accumulation de données à caractère personnel, utilisables dans des contextes très diversifiés, nuit au respect de la vie privée.

Toutefois, ce principe tend à être bafoué tant en Europe que dans le reste du monde, de sorte que les données à caractère personnel disponibles peuvent souvent être utilisées à d'autres finalités que celles initialement prévues, même si cette possibilité a été exclue lors du processus législatif. À titre d'exemple, des discussions sont en cours concernant l'utilisation des données relatives au péage pour l'application de la législation ou l'exploitation à des fins commerciales des données relatives à la conservation des informations dans le domaine des télécommunications. Or, cette tendance est amplifiée par le nombre croissant d'«identificateurs uniques» pouvant servir de «numéro d'identification personnel» (*Personenkennzeichen* ou PIN). En règle générale, ces identificateurs peuvent apparaître dans différents contextes d'application (par exemple, différents secteurs de la sphère gouvernementale ou lors de l'utilisation de l'internet pour différentes activités) et permettent d'identifier uniquement la personne qui se cache derrière le numéro en question. Le fait que des données à caractère personnel apparaissent dans des contextes divers permet d'établir des corrélations entre ces différentes sphères contextuelles et, partant, d'affiner sans cesse le profil de l'utilisateur. Ce phénomène a également été observé hors de l'Europe par des experts en matière de protection de la vie privée, dont Helen Nissenbaum qui parle d'«intégrité contextuelle» pour désigner le respect de la vie privée.

Disparités spécifiques

La disponibilité numérique croissante de données personnelles susceptibles d'être corrélées pose problème.

La disponibilité numérique croissante des données à caractère personnel, combinée aux possibilités toujours plus vastes de corrélation entre ces données, constitue un problème majeur. Même si ces données sont anonymes au départ, elles peuvent être mises en corrélation avec un profil susceptible de générer suffisamment d'informations pour permettre d'identifier la personne concernée. La capacité de corrélation (ou «corrélabilité») des données ne cesse de croître en raison, principalement, de l'usage répété d'identificateurs uniques qui sont souvent introduits par les systèmes TIC (adresses IP, *cookies* ou numéros d'indexation dans les bases de données). Cependant, la divulgation à plusieurs reprises d'informations telles que le nom est suffisante pour permettre aux moteurs de recherche d'accumuler des informations connexes.

Il est difficile de faire respecter le caractère contraignant de la finalité des données.

À moins que les données n'aient été prévues pour être utilisées dans un contexte spécifique[12], il apparaît difficile de faire respecter le caractère contraignant de la finalité des données. Néanmoins, l'application de ce principe peut être nettement facilitée par le recours au principe de la minimisation des données. Il existe plusieurs possibilités pour restreindre l'utilisation des données à un contexte spécifique, que ce soit au moyen d'identificateurs spécifiques à un secteur, dans le domaine de l'administration en ligne (voir l'exemple de la «carte du citoyen» (Bürgerkarte) en Autriche), par l'utilisation de pseudonymes différents selon les sites web ou la «pseudonymisation» des données à caractère personnel dans les bases de données, ou encore à l'aide de «*private credentials*» [justificatifs d'identité ou authentifiants] ou de «*minimum disclosure certificates*» [certificats minimaux de divulgation]. Les justificatifs d'identité permettent de prouver, avec un niveau accru de protection de la vie privée, les autorisations données et de responsabiliser l'utilisateur, tout en lui assurant l'anonymat, puisque ce dernier ne peut être identifié qu'en cas d'utilisation erronée. Ils mettent ainsi en œuvre des méthodes de responsabilisation des utilisateurs dans le monde en ligne, sans que ceux-ci soient tenus de communiquer leur véritable nom et des informations personnelles complémentaires à tous les partenaires avec lesquels ils interagissent.

Des solutions technologiques trop peu usitées.

Bien que toutes ces solutions soient abordées comme des composantes des systèmes de gestion de l'identité centrée sur l'utilisateur et qu'elles aient gagné en maturité au cours de ces dernières années, les concepts qu'elles véhiculent – et, en particulier, les approches plus sophistiquées concernant les justificatifs

[12] Nous laissons ouverte la discussion sur le degré de précision qu'il convient de donner au concept de la spécificité du contexte (ou «d'usage contextuel»). Dans certains domaines, chaque transaction peut refléter un contexte qui lui est propre, alors qu'une perspective plus générale sera davantage appropriée dans d'autres domaines. La notion de «finalité» pourrait servir de point de repère pour le débat sur les contextes, mais cette approche reviendrait aussi à négliger les dispositions réglementaires.

d'identité – demeurent encore mal connus et les concepteurs d'applications ne les emploient que rarement dans leurs systèmes TIC. De surcroît, le débat piétine, au sein de la société, au sujet des conditions de «corrélabilité» et de «non-corrélabilité» des données qu'il serait souhaitable de fixer car nombre de parties prenantes n'ont toujours pas pris conscience qu'il s'agit là d'un enjeu important ou n'ont pas connaissance des solutions possibles.

Solutions proposées

Défis en matière de R&D

Renforcer l'application concrète des concepts.

Bien que les concepts de distinction contextuelle et de gestion de l'identité centrée sur l'utilisateur aient acquis plus de maturité au cours de l'année dernière, des progrès restent encore à faire en termes d'intégration, d'interopérabilité et de facilité d'utilisation.

Mettre en place l'infrastructure requise pour les justificatifs d'identité.

Nous recommandons, en outre, que les administrations et les entreprises œuvrent à la mise en place des infrastructures nécessaires pour émettre des justificatifs d'identité, et – le cas échéant – qu'elles y aient recours dans leurs systèmes TIC.

Mesurer la corrélabilité des données.

Par ailleurs, des recherches devraient être menées sur la mesure du degré de «corrélabilité» ou de «non-corrélabilité » des données. Cette mesure est importante à la fois pour la conception des systèmes TIC et pour que l'utilisateur puisse garder le contrôle de sa sphère privée. En particulier, la question de savoir comment garantir la protection des données et maintenir la protection de la vie privée sur le long terme demeure, à ce jour, sans réponse.

Défis juridiques

Évaluation de la législation actuelle à la lumière des justificatifs d'identité.

La possibilité de disposer de technologies de distinction contextuelle a des implications sur l'interprétation du principe de la minimisation des données, selon lequel le traitement des données à caractère personnel ne devrait pas être excessif, mais devrait au contraire se limiter au strict minimum. Nous recommandons aux législateurs et aux décideurs politiques, tant au niveau national qu'européen, d'évaluer la législation actuelle à la lumière des justificatifs d'identité.

Défis en matière de communication

Ouvrir un débat de société sur la corrélabilité (ou non-corrélabilité).

Nous proposons d'attirer l'attention des décideurs politiques, des développeurs, des commissaires à la protection de la vie privée et des utilisateurs sur les conditions souhaitées en matière de corrélabilité (et non-corrélabilité) des données ainsi que sur les applications juridiques, organisationnelles et technologiques. Cette question se révèle particulièrement importante en ce qui concerne les concepts contre-intuitifs, tels que les justificatifs d'identité.

Liens

Brands, Stefan A., *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.

Camenisch, J., et Lysyanskaya, A., *Efficient Nontransferable Anonymous Multishow Credential System with Optional Anonymity Revocation*, rapport de recherche RZ 3295, n° 93341, IBM Research, novembre 2000.

Chaum, D., *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, Comm. ACM, vol. 28, n° 10, octobre 1985, p. 1030 à 1044.

Clauß, S., et Köhntopp, M., *Identity management and its support of multilateral security*, Computer Networks 37(2): 205-219, 2001.

Jøsang, A., et Pope, S., *User Centric Identity Management*, Proceedings of AusCERT, Gold Coast, mai 2005.

Nissenbaum, H., *Privacy as Contextual Integrity*, Washington Law Review, vol. 79, n° 1, 2004.

PRIME White Paper – Privacy and Identity Management for Europe, V3, https://www.prime-project.eu/prime_products/whitepaper/.

4.5 Informations sur les incidents en matière de sécurité

Les citoyens ne peuvent protéger efficacement leur vie privée que s'ils disposent d'informations suffisantes sur le traitement prévu des données, sur les risques y afférents pour la sécurité et la protection de la vie privée ainsi que sur les incidents survenus à cet égard et impliquant leurs données à caractère personnel.

Disparités spécifiques

Pas d'obligation d'informer les personnes concernées des atteintes à la sécurité et à la protection de la vie privée.

Dans le cadre de la législation européenne actuelle sur la protection des données, les responsables du traitement des données ne sont pas tenus d'informer les personnes concernées des incidents en matière de sécurité et de protection de la vie privée. Aux termes de l'article 4 de la directive 2002/58/CE[13], il est fait obligation au responsable du traitement des données de prendre des mesures de sécurité pour limiter les risques éventuels et d'informer l'utilisateur de ces risques, mais cette obligation concerne uniquement la période antérieure à la survenance d'un quelconque incident de sécurité. Aucune obligation de communication n'est prévue après qu'un incident a eu lieu.

Le législateur pensait sans doute que l'environnement compétitif et le processus d'autorégulation compléteraient le cadre juridique, grâce à la mise en œuvre des garde-fous techniques et organisationnels requis pour la gestion correcte des incidents en matière de sécurité. Or, ces premières mesures d'encouragement se révèlent insuffisantes pour stimuler la nécessité d'informer l'utilisateur final des violations de sécurité et d'atténuer, de façon proactive, leurs effets négatifs, si l'on en juge par les incidents graves et exemplatifs qui ont été constatés.

En outre, le manque, voire l'absence, de notification des incidents nuit à la mise en œuvre des mesures de prévention requises par le cadre juridique actuel.

Une autre conséquence directe de cette absence de notification et d'information sur les incidents en matière de sécurité est le manque de fiabilité des statistiques et données chiffrées qui sont produites, ce qui ne contribue nullement à créer un environnement davantage digne de confiance et plus transparent.

Même si des informations sont données sur la survenance d'une violation de la sécurité, la population ignore généralement comment elle pourrait être touchée par cette violation et comment y faire face de façon appropriée.

[13] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Solutions proposées

Défis en matière de R&D

Utiliser les messages d'information sur la sécurité comme format standard de rapport.

Conçu selon le modèle des *news feeds* [alimentation en nouvelles] destinés à faire rapport sur la vulnérabilité d'un système en matière de sécurité (tels que ceux communiqués par les *Computer Emergency Response Teams* [équipes d'intervention d'urgence informatique]), un prototype d'«alimentation en nouvelles de sécurité» a montré comment des informations sur les menaces et incidents en matière de sécurité et de protection de la vie privée peuvent être converties et transférées dans un format XML structuré via un dispositif d'alimentation RSS, puis interprétées par le système de gestion de l'identité mis au point dans le cadre du projet PRIME (*Privacy and Identity Management for Europe*). Ce concept inclut tous les mécanismes et dispositifs de mise en œuvre utilisés, tels que les protocoles, applications, algorithmes cryptographiques, de même que le logiciel de gestion de l'identité lui-même. Les utilisateurs sont informés, notamment, des risques d'ingérence dans leur sphère privée (qui a ou pourrait avoir un accès non autorisé à leurs données personnelles?) ainsi que des conséquences qui en découlent et des diverses mesures pouvant être prises.

Défis juridiques

Des dispositions juridiques doivent obliger les responsables du traitement des données à notifier les violations de sécurité.

Les responsables du traitement des données eux-mêmes devraient être tenus, juridiquement, d'informer les personnes concernées — que ce soit à titre individuel ou via les médias — des incidents en matière de sécurité, à l'instar des *Security Breach Notification Acts* [lois sur la notification des violations de sécurité] en vigueur dans de nombreux États américains.

En novembre 2007, la Commission européenne a publié une proposition[14] de modification de la directive 2002/58/CE et introduit l'obligation de notifier les violations de sécurité.

Les incidents relatifs au respect de la vie privée sont aussi dignes d'attention.

Il est à noter que le débat ne porte généralement que sur les incidents de sécurité, tels les opérations de piratage ou la perte de données. Cependant, d'autres événements peuvent se révéler pertinents pour le respect de la vie privée comme, par exemple, la fusion de différentes sociétés et leur participation conjointe à des bases de données, le transfert vers un autre pays du lieu de traitement des données à caractère personnel, etc. Ce genre d'information peut aussi être important en ce qui concerne le respect de la vie privée de la personne concernée.

[14] Proposition du 13 novembre 2007 de directive du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, et la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Défis en matière de communication

La notification des incidents permet aux citoyens de mieux gérer les aspects relatifs à leur vie privée.

Il convient de fournir aux personnes concernées des informations compréhensibles sur tous les incidents relatifs à la sécurité et à la protection de la vie privée qui peuvent les toucher ou impliquer leurs données. Des conseils devraient, en outre, leur être dispensés de manière individuelle quant aux mesures à prendre pour minimiser les effets indésirables sur leur vie privée. Ces informations favorisent la transparence des procédures de traitement des données ayant un impact réel sur la vie privée et servent de base à chaque individu pour la gestion de sa sphère privée.

Des rapports plus précis et exhaustifs sur les violations de sécurité permettraient d'encourager l'adoption de solides garde-fous après la survenance d'incidents ainsi que de mesures de compensation mûrement réfléchies pour gérer le risque résiduel.

La notification des incidents doit se faire via divers canaux de distribution.

Les informations disponibles sur les menaces ou incidents relatifs à la sécurité et à la protection de la vie privée devraient être diffusées non seulement par les responsables du traitement des données eux-mêmes, mais aussi par d'autres parties, telles que les médias écrits, les autorités chargées de la protection des données, les organisations de protection des consommateurs ou d'autres personnes concernées. Ces informations pourraient être transmises dans un format numérique normalisé, afin d'être aisément interprétées par l'ordinateur de l'utilisateur final. Leur combinaison avec des systèmes de gestion de l'identité contrôlée par l'utilisateur permettrait de créer des synergies.

Liens

Security Breach Notification Laws: Views from Chief Security Officers, étude menée pour la Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, décembre 2007, http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf.

Hansen, M., et Schallaböck, J., *Extending Policy Negotiation in User-Controlled Identity Management by Privacy & Security Information Services*, note de synthèse présentée à l'atelier de travail W3C «Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement», http://www.w3.org/2006/07/privacy-ws/papers/18-hansen-user-controlled-idm/.

Hansen, M., *Marrying Transparency Tools With User-Controlled Identity Management*. In: Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (Hrsg.): *The Future of Identity in the Information Society*, Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society, août 2007; IFIP International Federation for Information Processing, volume 262; Springer; 2008, p. 199 à 220.

Hogan & Hartson Analysys, *Preparing the Next Steps in Regulation of Electronic Communications – A Contribution to the Review of the Electronic Communications Regulatory Framework*, http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf.

Nageler, A., *Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem*, mémoire de fin d'études, Christian-Albrechts-Universität zu Kiel, mai 2006.

4.6 Orientations sur les systèmes de certification

Les systèmes de certification peuvent aider au contrôle de la conformité.

Un des principaux problèmes auxquels la société de l'information est aujourd'hui confrontée est le manque de transparence des produits et services TIC qui sont développés, quant à leur conformité aux normes de sécurité et de protection de la vie privée. Pour les utilisateurs, les responsables du traitement des données et les DPA, la conformité à ces normes représente donc un des défis majeurs des technologies de l'information et de la communication. Les schémas de certification doivent garantir qu'un produit ou un service a été conçu et peut être utilisé conformément à la législation européenne sur la protection des données.

Disparités spécifiques

Il n'existe, à l'heure actuelle, aucune certification en matière de protection de la vie privée.

Tous les acteurs au sein de l'Union européenne éprouvent le même besoin de pouvoir disposer de solutions TIC d'une totale fiabilité et, plus particulièrement, d'applications technologiques avancées en matière de sécurité et de protection des données. L'accent devrait, dès lors, être mis sur l'élaboration des mesures et critères nécessaires pour que des systèmes fiables de certification de la conformité aux normes de protection de la vie privée puissent être mis à disposition de façon harmonisée dans tous les États membres.

Les systèmes de certification renforcent l'efficacité des mesures de protection de la vie privée.

Dans la suite de cette section, nous nous attacherons à démontrer l'existence de cette disparité et à présenter les règles à respecter pour y remédier ainsi que les conséquences positives/bénéfices qui peuvent en être retirés. Parmi ces derniers, il y a lieu de citer notamment: des avantages concurrentiels, une confiance accrue dans des produits certifiés, un degré plus élevé de sensibilisation et de confiance du public, l'attention accordée au respect de la vie privée dès la conception plutôt qu'après coup et une application homogène – et, partant, plus efficace – des principes de protection des données pour tous les acteurs de la société de l'information (personnes concernées, responsables du traitement des données, autorités chargées de la protection des données, développeurs de systèmes TIC, vendeurs, fabricants, États membres, etc.).

Un niveau minimal de protection des données à caractère personnel devrait être fixé.

Nous tenons ici à souligner que: a) les systèmes de certification susmentionnés devraient, en fin de compte, garantir qu'un produit déterminé satisfait à un certain niveau (ou «niveau minimal») de protection des données à caractère personnel; b) il apparaît nécessaire d'élaborer une méthode pour atteindre cette finalité et pour promouvoir l'adoption de ces systèmes de certification; c) les organes de certification doivent normaliser les référentiels, les critères et les conditions de certification appliqués pour évaluer la conformité aux normes de protection de la vie privée.

Solutions proposées

Des mesures doivent être adoptées pour encourager la certification.

Les États membres devraient promouvoir et régir la mise en place de systèmes de certification, en impliquant aussi les associations de consommateurs. Ils devraient ainsi offrir des avantages fiscaux aux entreprises respectueuses de la vie privée, voire envisager l'exemption des sociétés de certaines obligations de déclaration à la condition qu'elles disposent d'une certification en matière de protection de la vie privée.

La réflexion doit porter, dans un premier temps, sur les questions suivantes: ce système de certification devrait-il être obligatoire ou facultatif? Qui devrait endosser l'adoption de ce système? Comment assurer la transparence lors des débats visant à obtenir un consensus général sur les exigences à satisfaire en matière de protection de la vie privée pour pouvoir remédier à la disparité susmentionnée? Il conviendra, dans un second temps, d'envisager de nouvelles solutions pour favoriser la conformité à ces exigences. À titre d'exemple, les États membres devraient concevoir des instruments permettant aux soumissionnaires qui répondent à un appel d'offres public de fournir, sur une base volontaire, une certification ou autocertification de leur conformité à la législation sur la protection des données.

Quelques expériences de systèmes de certification ont déjà été enregistrées.

Nous suggérons de nous inspirer des enseignements tirés de projets de recherche similaires (dont le projet EuroPriSe[15]) et d'autres pays (dont la Suisse[16]) qui ont mis au point des systèmes de certification de ce genre, de même que de l'expérience acquise par le passé dans les dispositifs agréés de signature électronique, les technologies liées au cryptage et leurs cadres juridiques respectifs.

[15] Voir http://www.european-privacy-seal.eu/.

[16] Voir l'ordonnance du Conseil fédéral suisse du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD), et la loi fédérale de l'Assemblée fédérale de la Confédération Suisse du 19 juin 1992 (État le 1er janvier 2008) sur la protection des données (LPD). Voir http://www.admin.ch/ch/f/rs/235_13/index.html.

Caractéristiques fondamentales d'un système de certification en matière de protection de la vie privée.

Ce type de système de certification devrait, selon nous, présenter les caractéristiques suivantes: les parties désireuses d'être reconnues par le grand public comme des organismes certificateurs agréés en matière de sécurité et de protection de la vie privée devraient au préalable être officiellement déclarées aptes à accomplir cette fonction par des tierces parties indépendantes, déjà établies en tant qu'organismes d'agrément dans ce domaine (travaillant en collaboration avec les DPA). Pour obtenir ce certificat d'agrément, les organismes devraient démontrer qu'ils satisfont aux exigences technologiques et juridiques (prise en compte du respect de la vie privée dès la conception, meilleures techniques disponibles, minimum de principes de protection de la vie privée) définies dans les règlements correspondants des DPA, en collaboration avec le groupe de travail «Article 29» et la Commission européenne. Ce certificat devrait être délivré pour une durée déterminée (n'excédant pas deux ou trois ans, par exemple), au cours de laquelle des évaluations annuelles de la conformité devraient être envisagées. Outre le retrait du certificat, des sanctions et amendes devraient être prévues en cas de violation ou d'utilisation abusive de ce certificat, de fausse déclaration ou de malversation. Il apparaît donc nécessaire que la Commission prenne de nouvelles mesures législatives en ce sens, de manière à faciliter la mise en œuvre et l'application harmonisées des systèmes de certification dans toute l'Union européenne. Il y a lieu, notamment, de définir les contrôles auxquels les évaluateurs et les organismes de certification seront soumis ainsi que la responsabilité qu'ils devront assumer.

Nécessité d'une normalisation internationale.

Enfin, les référentiels de certification devraient être normalisés au niveau international afin de garantir l'harmonisation et la transparence des méthodes utilisées et des critères pris en compte. Ces référentiels devraient contenir les critères dont le respect doit être apprécié lors de l'évaluation des produits ou services concernés. Ils devraient servir d'éléments d'orientation pour les évaluateurs chargés de contrôler la conformité des produits et services TIC.

4.7 Outils de surveillance

Des outils sont nécessaires pour procéder à des audits internes sur le respect de la vie privée.

Les entreprises qui traitent des données à caractère personnel doivent préciser leur politique en matière de protection de la vie privée et s'assurer que celle-ci est correctement mise en œuvre dans leur environnement. Cette politique peut, de fait, se révéler très complexe du fait du grand nombre de paramètres à prendre en considération et, une fois appliquée, elle devrait faire l'objet de contrôles continus, automatisés et modulables. Cependant, aucun instrument de surveillance et de gestion n'est mis à la disposition des entreprises et celles-ci manquent d'outils efficaces pour effectuer des audits internes sur le respect de la vie privée.

En outre, les autorités chargées de la protection des données (DPA) sont confrontées en permanence à des difficultés pour effectuer des contrôles et mener des audits sur les données à caractère personnel qui sont enregistrées, traitées et exploitées. Enfin, bien que le cadre juridique européen définisse, de façon détaillée, les obligations et mesures de protection que les responsables du traitement des données doivent mettre en place et respecter[17], il ne fournit pas pour autant des outils de surveillance concrets et n'exige pas que de tels outils soient développés en faveur des autorités de contrôle.

Les autorités de protection des données ont aussi besoin d'instruments adéquats.

Disparités spécifiques

La plupart des systèmes TIC qui traitent des données à caractère personnel ne sont généralement pas conçus pour faciliter les contrôles, ni même les activités d'auto-vérification. Les outils de surveillance doivent donc être adaptés au cas par cas, ce qui nécessite des ressources supplémentaires ainsi qu'une réelle aptitude à vérifier la conformité de mesures concrètes de protection de la vie privée à une politique de haut niveau en la matière. Pour ce faire, des dispositifs métrologiques dédiés à la protection de la vie privée doivent être utilisés et certaines fonctions doivent être incluses pour le contrôle des correspondances entre les spécifications de haut niveau et les configurations matérielles au sein du système d'information.

Procéder à un audit sur le respect de la vie privée exige de nombreuses ressources.

Par ailleurs, il apparaît essentiel, compte tenu de l'ampleur des activités de collecte de données à contrôler, de mettre au point des techniques normalisées et irréfutables d'enregistrement chronologique (journalisation) des données, afin de permettre des vérifications automatisées et fiables.

Il pourrait ensuite être envisagé de mettre ces outils à la disposition des DPA, si possible en les dotant d'une fonction d'accès à distance, car ceux-ci pourraient aider les DPA à exercer leurs pouvoirs d'inspection sur une base continue. De même, l'utilisateur final devrait aussi être en mesure d'obtenir automatiquement des informations sur la façon dont ses données personnelles sont traitées.

Des outils de surveillance seraient utiles à la fois pour les entreprises, les DPA et les utilisateurs.

Solutions proposées

Défis en matière de R&D

Les politiques de protection de la vie privée pourraient être appliquées aux données transférées (par exemple, en les «encapsulant» dans ces données) de sorte qu'elles ne puissent pas en être dissociées («*sticky policies*») et que les responsables du traitement des données soient obligés de respecter les dispositions y contenues. Pour des raisons de transparence, cette pratique nécessite non seulement d'indiquer les catégories générales de destinataires (comme la législation l'impose aujourd'hui), mais aussi de préciser quels sont les véritables destinataires.

Programmation paradigmatique des «*sticky policies*».

[17] Voir, à titre d'exemple, l'article 17 de la directive 95/46/CE.

Synchroniser les composantes techniques et juridiques des politiques de protection de la vie privée.

Des outils automatisés et efficaces de contrôle des pratiques mises en œuvre en matière de protection des données faciliteraient l'application des politiques. Des pistes de vérification pourraient être incluses, de façon proactive, dans les systèmes, afin de permettre la décompilation (ou «ingénierie inverse») de la composante technique d'une politique de protection de la vie privée et vérifier que cette dernière se conforme à des exigences de protection d'un niveau élevé.

Il convient, en outre, d'encourager les travaux de recherche et développement en vue d'accroître l'offre d'instruments automatiques de contrôle, de traçabilité et d'audit. Le cas échéant, ces travaux pourraient aussi être confiés à des organismes (privés) agréés, capables de mener de telles activités et de délivrer des certificats aux organisations qui satisfont aux exigences de respect de la vie privée (voir, par exemple, le système de certification mis en place dans le canton de Genève, en Suisse).

Des points de contrôle déterminés simplifient les vérifications.

La détermination de points de contrôles précis (et, si possible, normalisés) dans les systèmes TIC et de flux de traitement des données faciliterait le travail tant des auditeurs internes (tels que les membres du département d'audit) que des auditeurs externes (tels que les autorités chargées de la protection des données). De plus, les procédures d'essai utilisées lors d'un audit devraient couvrir tous les cas pertinents. Aux fins d'une surveillance à long terme, il pourrait même être envisagé d'introduire certaines données fictives pour voir s'il ne se produit pas une fuite de ces données et si celles-ci ne réapparaissent pas, par la suite, hors du système TIC. En pareille hypothèse, il conviendra d'être extrêmement attentif à ce que ces données fictives d'essai n'évoluent pas au point de devenir une identité numérique incontrôlée susceptible d'être utilisée abusivement.

Défis juridiques

Exiger des pistes de vérification tout au long du cheminement des données.

Il serait possible d'imposer, juridiquement, que le traitement des données à caractère personnel ne soit autorisé que si les données proviennent d'une source fiable et si tous les transferts des données ont été dûment documentés.

Accès à distance pour les DPA.

Il y aurait lieu d'examiner la possibilité de doter les DPA d'un accès permanent et à distance à un nombre limité de fonctions des outils de surveillance du respect de la vie privée qui sont utilisés par les responsables du traitement des données. Les DPA pourraient, de la sorte, vérifier que les systèmes respectent les notifications et les inspections en seraient facilitées.

Défis en matière de communication

Essais internes grâce à des procédures d'autocertification.

L'établissement de rapports d'autocertification aiderait, en outre, les autorités de surveillance à exécuter efficacement leurs tâches car elles pourraient ainsi identifier les points les plus faibles et se focaliser sur ceux-ci durant leur propre procédure d'audit.

4.8 Orientations sur les meilleures techniques disponibles

La sécurité et la protection de la vie privée posent des problèmes complexes qu'il semble difficile de résoudre une fois pour toutes par le simple recours à une solution technique universelle. Au contraire, chacun des différents domaines d'application requiert un soutien technique différent pour assurer la protection de la vie privée des citoyens. En outre, ce soutien technique doit être soigneusement complété par un cadre juridique et des directives pratiques, ciblant un domaine d'application particulier ou un ensemble déterminé de principes opérationnels. Cette combinaison particulière de technologies, de protocoles, de normes, de pratiques, etc. – qui permet d'assurer un niveau raisonnable de protection de la vie privée dans un domaine particulier – peut être désignée par l'expression «meilleures techniques disponibles» (MTD).

Les MTD représentent une combinaison particulière de technologies, de protocoles et de normes.

Disparités spécifiques

Les meilleures techniques disponibles ne font toujours pas l'objet d'une définition unique et d'une harmonisation au niveau européen. Il convient de remédier à cette lacune en déterminant quelles sont les meilleures techniques disponibles dans les différents domaines et en précisant dans quelle mesure celles-ci devraient ou doivent être utilisées par les responsables du traitement et les sous-traitants.

Il importe de déterminer et d'harmoniser les MTD en matière de sécurité et de protection de la vie privée.

Le débat actuel concernant les techniques de protection des données relatives à la localisation est assez révélateur du problème existant. Bon nombre des propositions actuelles de protection de ces données tentent de cacher les demandes de localisation dans un domaine suffisamment large pour contenir au moins *k-1* autres utilisateurs. C'est ce que l'on appelle le «k-anonymat». Si cette fonction donne de bons résultats, il est néanmoins important de se pencher plus spécifiquement sur le problème de l'utilisation pratique de ces techniques: comment un utilisateur peut-il employer une technique, disons, de «k-anonymat»? Comment déterminer quelle est la valeur appropriée de *k*? Comment savoir quand il y a lieu d'activer ou de désactiver le système? Comment trouver le juste équilibre entre la nécessité de préciser la localisation et celle de protéger les données relatives à cette localisation? Devrions-nous simplement adopter un modèle éprouvé, basé sur l'intervention d'une tierce partie et impliquant la gestion centralisée de toutes les données (par le fournisseur de téléphonie mobile, par exemple), ainsi que des approches axées sur l'utilisation de bases de données statistiques et d'autres outils pour protéger les profils des utilisateurs? Des scénarios d'application différents appellent sans doute des réponses différentes.

Exemple de la protection des données relatives à la localisation.

Solutions proposées

Déterminer un ensemble de MTD dans le domaine de la protection des données nécessite à la fois de trouver les techniques qui conviennent et de mettre en place un processus d'harmonisation de ces techniques dans tous les États membres de l'Union européenne.

Défis en matière de R&D

Identifier et regrouper les technologies et les pratiques.

La première étape consiste à repérer les ensembles d'applications pertinents et, en particulier, ceux liés au développement de technologies nouvelles (ex.: RFID, services basés sur la localisation, biométrique, …). Ceux-ci pourraient ensuite être regroupés en fonction de leurs modèles respectifs de flux d'information, c'est-à-dire leurs pratiques particulières de traitement des données et leurs besoins en information.

Déterminer des groupes de techniques adaptés à chacun des domaines spécifiques d'application.

Après avoir déterminé les différents types d'applications génériques, il conviendra de passer en revue les technologies et pratiques existantes, de manière à établir une palette précise des meilleures techniques disponibles pour chacun de ces types. Comme indiqué ci-dessus, la viabilité économique et technique constitue un critère d'évaluation essentiel.

Défis juridiques

Faire participer les DPA et définir des modèles d'application.

Les autorités chargées de la protection des données (DPA) doivent être invitées à participer au processus d'identification et d'énumération des MTD en matière de sécurité et de protection de la vie privée. Il conviendra, toutefois, de déterminer dans quelle mesure les DPA peuvent et doivent imposer le recours à ces MTD, notamment dans le cas où certaines technologies sont disponibles mais ne font pas partie intégrante des systèmes standard (ex.: suppression sûre des données à l'aide d'outils d'effacement non intégrés dans les systèmes opérationnels standard) ou lorsque leur usage nécessite soit la coopération de plusieurs parties, soit une infrastructure complémentaire (ex.: les systèmes d'anonymisation — qui visent à protéger des données à caractère personnel avant qu'elles ne puissent être détectées par un responsable du traitement des données — ne peuvent pas être utilisés par le seul responsable, mais requièrent l'intervention d'autres fournisseurs indépendants).

Anticiper les futures combinaisons technologiques.

Les solutions proposées doivent prendre en considération les risques générés par la combinaison de plusieurs technologies existantes; en d'autres termes, ces risques doivent être anticipés, analysés et quantifiés. À titre d'exemple, la combinaison de systèmes biométriques de reconnaissance du visage avec des outils de surveillance vidéo ou de services basés sur la localisation avec des données cartographiques peut engendrer des risques considérables. Lors de l'élaboration d'une politique relative à une technologie spécifique, il est donc important de prévoir quels en seront les usages futurs, de sorte que des dispositifs adéquats de limitation des finalités puissent être inclus à chaque phase de la conception de la technologie en question.

Défis en matière de communication

La liste des MTD choisies pour des groupes majeurs d'applications ainsi que leurs caractéristiques respectives doivent être diffusées auprès du public, afin que chaque responsable du traitement et chaque sous-traitant en aient connaissance. Les meilleures pratiques pourraient aussi illustrer l'usage qui peut être fait des MTD.

Une procédure publique.

Liens

La directive 96/61/CE relative à la prévention et à la réduction intégrées de la pollution[18] a fourni une définition satisfaisante des MTD dans le domaine de l'environnement.

Le BSI (Bundesamt für Sicherheit in der Informationstechnik; office fédéral allemand pour la sécurité des informations) a lancé récemment un projet qui constitue un exemple intéressant de MTD dans le domaine des applications RFID[19].

4.9 Mesures d'incitation et sanctions efficaces

Bien que la législation sur la protection des données s'appuie sur des bases anciennes, la conformité des systèmes TIC et des structures organisationnelles à cette législation fait souvent défaut dans le cadre des activités actuelles de traitement des données. Comme nous avons pu le constater au cours des dernières décennies, les technologies renforçant la protection de la vie privée ne peuvent pas évoluer à grande échelle lorsque tout repose sur les seules forces libres du marché.

La législation sur la protection de la vie privée est rarement respectée.

Disparités spécifiques

Force est de constater que, dans l'ensemble, les responsables du traitement des données ne sont pas suffisamment motivés à respecter la législation sur la protection des données. À cela, il convient d'ajouter un autre constat – étroitement lié au précédent – à savoir, le manque de motivation à utiliser les technologies renforçant la protection de la vie privée, lesquelles permettraient pourtant de faire évoluer l'état de la technique.

La motivation fait défaut et les mesures d'encouragement sont insuffisantes.

[18] Voir http://ec.europa.eu/environment/air/legis.htm#stationary.
[19] Voir http://www.bsi.de/presse/pressinf/071207_RFID.htm.

De manière générale, un cas de non-conformité ne peut être sanctionné que si l'infraction à la législation sur la protection des données est portée à la connaissance de l'autorité de surveillance ou d'une juridiction compétente. À l'heure actuelle, les autorités de protection des données ne peuvent contrôler qu'un petit nombre de responsables du traitement, de sorte que les infractions à la législation passent souvent inaperçues.

Le manque d'outils ne permet pas aux DPA de contrôler valablement la conformité à la législation.

Qui plus est, les mesures économiques destinées à inciter ces mêmes responsables à observer les dispositions juridiques en vigueur se révèlent souvent insuffisantes, compte tenu de la légèreté des sanctions prévues. C'est ainsi que, dans certains États, les responsables du traitement des données ne peuvent être sanctionnés qu'une seule fois: même s'ils ne changent rien à la façon dont ils traitent les données, une seule amende leur sera infligée. Dans diverses affaires, les tribunaux ont même fermé les yeux sur l'obligation pour les contrevenants de payer une amende, pour éviter de devoir contrôler tous les concurrents du responsable en cause, lorsqu'ils ont été confrontés à des accusations de discrimination.

Les mesures d'incitation à observer la législation sont insuffisantes au regard des enjeux économiques d'aujourd'hui.

Solutions proposées

Pour encourager les responsables du traitement des données à renforcer la protection de la vie privée des personnes concernées, deux options sont possibles:

Renforcer la conformité à la législation par l'octroi de récompenses ou l'application de sanctions.

1. offrir des *incitations* pour récompenser le responsable du traitement des données;
2. appliquer des *sanctions* pour punir le responsable du traitement des données.

Le choix entre une incitation et une sanction dépendra du type de responsable du traitement concerné. Pour les entreprises, les moteurs économiques priment. Dès lors, si une amende doit être infligée à une entreprise pour sanctionner le fait qu'elle ne se conforme pas à la législation sur la protection des données, elle devra être suffisamment conséquente pour l'entreprise concernée, afin de ne pas se limiter à acquitter cette dernière des atteintes portées à la vie privée. S'agissant des administrations publiques, le traitement des données *doit* se conformer à la législation sur la protection des données, sinon les mécanismes de surveillance réglementaire devront être immédiatement activés.

Pour être efficaces, les sanctions doivent être différentes pour les organismes publics et privés.

Défis en matière de R&D

Le manque d'instruments de contrôle automatisés restreint fortement les possibilités de faire appliquer la législation et, partant, de lutter contre les infractions. Pour mettre au point de tels instruments et établir ainsi une piste de vérification, il conviendrait de lancer un processus de normalisation et de certification afin de déterminer, en collaboration avec les autorités chargées de la protection des données, l'ensemble des informations requises.

Des outils d'audit normalisés sont nécessaires pour pouvoir vérifier efficacement la conformité.

Défis juridiques

Certification obligatoire ou utilisation de technologies renforçant la protection de la vie privée.

Les conditions inhérentes à la passation de marchés dans les services publics pourraient inclure une conception respectueuse de la vie privée ou une certification/autocertification. Certaines mesures technologiques pourraient être rendues obligatoires (comme c'est déjà le cas dans certains États), bien qu'il reste encore à définir quelles mesures seraient les plus intéressantes.

Des sanctions économiques effectives et significatives.

L'application de sanctions effectives pourrait contribuer à convaincre les responsables du traitement des données de mettre en œuvre des systèmes respectueux de la vie privée. Les sanctions ne doivent pas être seulement de nature administrative (dans certains États, des sanctions sont aussi prévues par le droit pénal), mais devraient inclure un système de responsabilité efficace. En pareil cas, les associations de consommateurs peuvent jouer un rôle important.

Toutefois, dans de nombreux États, le système de sanctions ne donne pas les résultats escomptés et devrait être couplé à un système d'audit performant. Par ailleurs, il conviendrait de prévoir aussi des mesures d'incitation, pouvant prendre la forme d'avantages fiscaux, par exemple. Pareilles mesures nécessitent et doivent être étroitement liées à un système de certification.

Nous recommandons à la Commission européenne et aux États membres d'encourager l'adoption de mesures d'incitation associées à un programme de certification ainsi que d'un système efficace de sanctions économiques.

Défis en matière de communication

Engager des campagnes pour susciter une demande de conformité à la législation auprès des consommateurs.

La conformité à la législation sur la protection de la vie privée ou la conception (dûment prouvée) du système de traitement selon des critères propres à renforcer la protection de la vie privée peut représenter un formidable argument de vente pour un responsable du traitement des données et lui permettre, en outre, de se forger une bonne réputation qui l'aidera à attirer et à fidéliser des clients. Par ailleurs, des campagnes de sensibilisation à la protection de la vie privée pourraient contribuer à susciter une demande du marché pour des systèmes respectueux de la vie privée, en particulier si les clients peuvent disposer de moyens aisés d'exprimer leurs souhaits à cet égard. Qui dit «moins de données à caractère personnel» dit aussi «moins de risques d'utilisation abusive», ce qui ne peut être que positif pour la réputation du responsable du traitement des données.

Expliquer les avantages des données anonymes.

Il importe de convaincre les responsables du traitement qu'une organisation du traitement des données axée sur le renforcement de la protection de la vie privée est souvent moins coûteuse — surtout lorsqu'elle se conforme au principe de la minimisation des données — qu'une autre organisation qui doit non seulement fournir des moyens de stockage des données, mais aussi des garde-fous appropriés, de la documentation et un accès aux personnes concernées (ou garantir l'application de la législation).

Liens

Sur son site web, Ross Anderson tient à jour une page intitulée *Economics and Security Resource* [Économie et ressources en matière de sécurité][20]. Alessandro Acquisti propose un site similaire sur l'économie de la protection de vie privée[21].

4.10 Données à caractère personnel ou à caractère non personnel?

La notion de données à caractère personnel couvre toutes les informations pouvant être liées à une personne physique.

Aux termes de la directive 95/46/CE, l'expression «données à caractère personnel» désigne toute information concernant une personne physique identifiée ou identifiable (personne concernée). Cette notion est suffisamment vaste pour couvrir toutes les informations susceptibles d'être liées à un individu. En réalité, beaucoup de données différentes peuvent être combinées entre elles et permettre ainsi d'identifier une personne donnée (que ce soit par le biais de réseaux sociaux, par le contrôle d'étiquettes RFID, en associant diverses questions formulées sur différents moteurs de recherche, ou par d'autres moyens). Aussi large soit-elle, la notion de «donnée à caractère personnel» adoptée par les législateurs européens n'est pas pour autant illimitée. Si la portée des règles de protection des données ne doit pas être étendue à l'infini, il convient cependant d'éviter de restreindre indûment le concept même des données à caractère personnel. La frontière entre «caractère personnel» et «caractère non personnel» d'une donnée étant parfois assez floue, des efforts ont été déployés pour tenter de clarifier cette notion, comme ce fut le cas du groupe de travail «Article 29» dans son avis sur le concept de données à caractère personnel.

Disparités spécifiques

Il n'est pas toujours aisé de déterminer si une donnée revêt ou non un caractère personnel.

Malgré les tentatives récentes du groupe de travail susmentionné, la notion de «donnée à caractère personnel» est encore souvent contestée. Ce manque de clarté pose problème car il est à craindre que les garde-fous adoptés dans le cas de données ne revêtant pas, *a priori*, un caractère personnel soient insuffisants pour empêcher que ces données n'acquièrent, en définitive, un tel caractère.

Exemple: lors de la vente au détail, les étiquettes RFID ne sont pas désactivées, même si elles n'ont aucune finalité en dehors du point de vente.

Par ailleurs, la perception que l'utilisateur a des données à caractère personnel et la notion d'intrusion acceptable dans la vie privée d'un individu sont des concepts dynamiques. À titre d'exemple, la technologie RFID est aujourd'hui utilisée dans le cadre de nombreuses applications (telles que la vente au détail, l'identité numérique dans les passeports, les clés de voiture, les services de paiement mobile, etc.). Cette technologie fait peser de nombreuses menaces,

[20] Voir http://www.cl.cam.ac.uk/~rja14/econsec.html.
[21] Voir http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

dans la mesure où elle pourrait permettre de surveiller un utilisateur et de collecter des données à son sujet quasiment partout, sans même que la personne concernée le sache. La technologie RFID permet, en effet, d'identifier une personne physique dès lors que des données relatives au nom de la personne ou des données biométriques sont enregistrées sur l'étiquette. Elle permet, en outre, de repérer une personne, de suivre sa trace et d'établir son profil à l'aide des étiquettes contenant une série de numéros uniques qui sont apposées sur les articles qu'elle porte. Lors d'une vente au détail, l'étiquette n'est généralement pas désactivée sur le lieu de vente car les données contenues dans cette étiquette sont utilisées à des fins de logistique et n'ont donc pas, en règle générale, vocation à revêtir un caractère personnel. Tout acheteur porte donc sur lui des articles pourvus d'étiquettes actives qui pourraient être exploitées pour suivre sa trace.

Qui plus est, il y a lieu de relever l'évolution, au fil du temps, de la perception que les utilisateurs ont des notions de «données à caractère personnel» et d'«intrusion acceptable dans leur vie privée», en fonction des facteurs sociaux, des exigences escomptées en matière de sécurité et des progrès technologiques. Les facteurs sociaux influent sur les réactions que chacun peut avoir à l'égard des technologies portant atteinte à la vie privée, étant donné que la définition de «sphère privée» est subjective et dépend de l'âge, de la culture et de l'environnement de la personne concernée. Les exigences escomptées en matière de sécurité diffèrent aussi, dans la mesure où il y a fort à parier que les utilisateurs expérimentés veuillent configurer leurs systèmes selon des paramètres précis, tandis que la majorité des utilisateurs préfère s'en tenir à des paramètres par défaut simples, compréhensibles et conformes aux règles de protection de la vie privée. Enfin, des données considérées aujourd'hui comme ne revêtant pas un caractère personnel (car les moyens requis pour leur conférer un tel caractère sont excessifs) pourraient acquérir un caractère personnel si l'évolution technologique devait rendre ces moyens raisonnables.

Solutions proposées

Défis en matière de R&D

Mettre au point des garde-fous technologiques appropriés, même pour les données n'ayant pas vocation à revêtir un caractère personnel.

Pour évaluer les risques d'atteinte à la vie privée qui sont inhérents au traitement des données, des méthodes d'évaluation des incidences sur la vie privée doivent être élaborées et appliquées. Le niveau de complexité de l'analyse à mener dépendra de la sensibilité du traitement et des données concernées.

Des garde-fous doivent être mis au point pour protéger adéquatement les données, que celles-ci revêtent ou non un caractère personnel. Cette mesure contribuera à améliorer notablement le niveau de responsabilisation des utilisateurs et le contrôle qu'ils peuvent exercer.

Lors de la conception de systèmes et l'élaboration de dispositions réglementaires, il convient d'anticiper de façon appropriée les évolutions technologiques et les moyens futurs, de sorte que les données qui ne sont pas

prévues pour revêtir un caractère personnel ne puissent pas acquérir ce caractère à la suite de progrès technologiques.

L'impact social des nouvelles technologies doit être évalué de façon systématique et scientifique, et leur utilité doit être démontrée.

Défis juridiques

La législation devrait garantir que des données à caractère non personnel ne puissent pas acquérir un caractère personnel.

La législation doit garantir une protection adéquate des données, en particulier s'il existe (ou s'il peut exister à l'avenir) un risque que celles-ci acquièrent un caractère personnel.

Toutefois, le droit à l'anonymat – en tant que forme d'exercice du droit au respect de la vie privée et du droit à la protection des données – doit être mis continuellement en balance avec d'autres droits fondamentaux. Dans la mesure où l'anonymat absolu n'est, en général, pas possible, d'autres formes d'anonymat «raisonnable» doivent pouvoir se développer.

Des mécanismes appropriés d'anonymisation des données devraient être utilisés dans la mesure du possible, notamment s'il s'agit de données sensibles.

Dès lors que la législation a établi un droit, en le mettant en balance avec d'autres droits, la technologie doit appliquer les règles qui s'y rapportent. L'effet utile d'un droit à l'anonymat doit être garanti par la technologie, laquelle doit offrir des mécanismes de protection adaptés à différents degrés d'anonymat.

La nécessité de procéder à une évaluation des incidences sur la vie privée pourrait être prévue dans la législation.

Lorsqu'une évaluation des incidences sur la vie privée fait apparaître des risques importants liés au traitement de données, le législateur devrait imposer la mise en œuvre de mesures appropriées de protection de la vie privée, afin de limiter ces risques.

Défis en matière de communication

La conscientisation des citoyens de l'UE permettra de modérer les risques qu'ils encourent dans le monde en ligne.

Le recours à des campagnes de sensibilisation contribuera à améliorer les pratiques des utilisateurs et, partant, à limiter les risques encourus par les citoyens de l'Union européenne dans le monde en ligne, en les aidant à mieux appréhender les technologies qui responsabilisent l'utilisateur et en attirant leur attention sur la nécessité de protéger leurs données.

Grâce à l'utilisation systématique de méthodes et procédures d'évaluation des incidences sur la vie privée, les entreprises rehausseront le niveau de transparence, réduiront les risques d'atteinte à la vie privée qui sont liés aux données qu'elles traitent et tireront profit de la confiance accrue que les utilisateurs accorderont à la technologie.

De plus, les campagnes de sensibilisation généreront un besoin, au sein de la population, de technologies efficaces et compréhensibles qui renforcent la protection de la vie privée.

Liens

La directive 95/46/CE[22] définit ce qu'il y a lieu d'entendre par «données à caractère personnel» ainsi que le cadre juridique correspondant.

Le concept de données à caractère personnel a fait l'objet de clarifications et d'un examen approfondi en 2007, dans le cadre d'un avis du groupe de travail «Article 29»[23].

4.11 Protection de la vie privée et tri social

Le tri social peut porter atteinte à la vie privée des citoyens, même si les données traitées n'ont pas un caractère personnel.

Dans de nombreux cas, les responsables du traitement des données n'ont pas pour objectif d'identifier individuellement les personnes au moyen de leurs données à caractère personnel («identification unique»), mais se focalisent plutôt sur des groupes de personnes, en vue d'établir une sorte de catégorisation. Cette opération – connue également sous les noms de «tri social», «stratification», «segmentation» ou «classification» – peut être effectuée à l'aide de techniques de profilage ou d'évaluation par score et à des fins diverses: marketing, détermination de la solvabilité, discrimination par les prix ou prises de décision dans des domaines aussi divers que le recrutement électronique, le secteur de la santé ou les enquêtes criminelles. En pareils cas, les données ne sont pas considérées comme revêtant, par elles-mêmes, un caractère personnel car elles ne sont pas liées à des individus particuliers. En d'autres termes, les responsables du traitement ne connaissent pas les noms des personnes dont les données sont traitées. Toutefois, ces opérations de collecte et d'analyse des données ont souvent des répercussions sur les personnes concernées et, partant, affectent leur vie privée. Or, la directive 95/46/CE sur la protection des données n'a pas prévu que les dispositions de son article 15, concernant les décisions individuelles automatisées, puissent couvrir tous ces différents cas.

[22] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

[23] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf

Disparités spécifiques

Manque de transparence du tri social pour les personnes concernées.

La principale lacune constatée en matière de tri social tient au fait que les personnes concernées n'ont souvent pas conscience de faire l'objet d'un tel tri et ignorent comment des décisions spécifiques les concernant sont adoptées. Autrement dit, elles ne savent ni si les données sur lesquelles le tri social se fonde sont correctes, ni si les algorithmes, les applications de l'évaluation par score et autres outils d'analyse utilisés fonctionnent adéquatement. En particulier, il se peut que l'entité qui génère les décisions relatives à des personnes ne soit pas la même que celle qui collecte et rassemble les informations, ce qui risque d'entraver les tentatives éventuelles, de la part de ces personnes, de porter plainte et d'obtenir réparation. Qui plus est, les personnes concernées n'ont généralement pas la possibilité de prouver que les prévisions contenues dans des scénarios prédictifs sont erronées.

L'exercice, à titre individuel, des droits au respect de la vie privée se révèle impossible dans le cas de données ne revêtant pas un caractère personnel.

Lorsque les données traitées ne sont pas considérées comme revêtant un caractère personnel, les chances sont faibles qu'une personne puisse exercer, à titre individuel, ses droits au respect de la vie privée (accès, rectification, effacement des données à caractère personnel si celles-ci sont stockées illégalement, révocation du consentement). Il faudrait, en effet, que la personne concernée puisse fournir la preuve que les données en question n'appartiennent qu'à elle seule. Dans divers cas, des individus se sont vu refuser le droit d'accès à des données relatives à des *cookies*, au motif qu'un *cookie* n'est pas nécessairement lié à un seul et unique individu. Cet exemple montre donc que beaucoup d'identificateurs jouissent de liens d'une qualité suffisante pour produire les informations désirées par l'entité chargée du traitement, mais ne permettent pas aux personnes concernées d'exercer leurs droits au respect de la vie privée.

L'accessibilité peut faciliter la manipulation directe.

Par ailleurs, certains paramètres permettent d'établir un contact avec un individu ou de l'atteindre directement, que ce soit par téléphone, en lui transmettant un message électronique ou une publicité personnalisée, ou encore via la télévision ou un site web. À cet égard, les formes de marketing visant à séduire les clients potentiels peuvent être particulièrement manipulatrices et porter atteinte à la vie privée d'une personne. Elles peuvent aussi provoquer des réactions qui permettront à l'entité chargée du traitement d'affiner les données collectées ou d'établir des liens à caractère personnel.

Solutions proposées

Le droit à l'autodétermination de l'information ne peut être exercé que si les personnes sont mises au courant de toutes les opérations de traitement de données qui les concernent.

Défis en matière de R&D

Une piste de vérification complète couvrant l'ensemble des opérations de traitement des données.

Une solution éventuelle consiste à établir un cadre organisationnel et technique garantissant aux personnes concernées la possibilité de se protéger et d'exercer leurs droits. Ce cadre pourrait imposer l'élaboration d'une piste de vérification complète à chaque fois que des données sont traitées, que celles-ci revêtent ou non un caractère personnel. La transparence de chacune des étapes du traitement des données – incluant toutes les entrées et sorties de données, dont les informations relatives aux parties responsables des données, algorithmes et mises en œuvre – pourra ainsi être assurée aux personnes concernées ou aux parties chargées par ces dernières de les représenter. De la sorte, les données incorrectes ou les failles existantes dans le système de traitement des données pourront être décelées et corrigées plus aisément.

Le cadre organisationnel et technique apparaît d'autant plus nécessaire si l'on songe à l'évolution de l'environnement ambiant où une foule de capteurs communiquent entre eux et collectent des informations sur ce qui les entoure, y compris les individus. À cet égard, les technologies renforçant la transparence pourraient aider les personnes concernées [Hildebrandt/Koops, 2007].

Défis juridiques

Un cadre juridique cohérent pour toutes les opérations de traitement des données susceptibles de nuire à des personnes.

À l'heure actuelle, les dispositions réglementaires censées remédier à la lacune susmentionnée semblent quelque peu disséminées: certaines s'inscrivent dans le cadre de la législation sur la protection des données, d'autres dans la législation sur la non-discrimination et d'autres encore ne s'intègrent dans aucune législation à part entière. En conséquence, le principal défi juridique à relever consiste à élaborer un cadre juridique cohérent et global qui prenne en compte tous les types de traitement de données à caractère personnel et non-personnel susceptibles de porter atteinte à des personnes. Ce cadre devrait inclure, tout particulièrement, l'obligation d'accroître la transparence et de rendre les opérations de traitement des données intelligibles pour les personnes concernées.

Défis en matière de communication

Informer les personnes sur la collecte et l'analyse de données.

Il importe de conscientiser les personnes sur les conséquences que peut avoir le fait de laisser involontairement des traces de données: lorsque cela se produit, elles doivent recevoir des informations indiquant quelles sont les données les concernant qui sont collectées et corrélées à d'autres données par différentes parties, ou dans quelles circonstances elles peuvent être tenues responsables – peut-être à tort – d'actions particulières. Elles doivent, en outre, être informées sur la meilleure manière de réagir si elles estiment faire l'objet d'un traitement inéquitable, eu égard à leur vie privée.

Liens

Hildebrandt, M., et Gutwirth, S., (Eds.), *D7.4: Implications of profiling practices on democracy and rule of law*, FIDIS Deliverable, Francfort a.M.,

Allemagne, septembre 2005, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf.

Hildebrandt, M., et Koops, B.-J., (Eds.), *D7.9: A Vision of Ambient Law*, FIDIS Deliverable, Francfort a.M., Allemagne, octobre 2007, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf.

Lessig, L., *Code and other laws of cyberspace*, Basic Books, New York, 1999.

Lyon, D., *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, Routledge, 2002.

Phillips, D. J., *Privacy policy and PETs – The influence of policy regimes on the development and social implications of privacy enhancing technologies*, New Media & Society, vol. 6, n° 6, SAGE Publications, Londres, Thousand Oaks, CA et New Delhi, 2004, p. 691 à 706.

Groupe de travail «Article 29»: avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, 01248/07/FR, WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf.

4.12 Respect de la vie privée, protection des données et notion d'«espace»

Le domaine numérique doit être mieux délimité.

La protection territoriale joue, depuis longtemps, un rôle majeur dans la protection de la vie privée («ma maison est ma forteresse»). Un territoire représente, généralement, un continuum dans l'espace. Il se peut néanmoins que les éléments réels et numériques afférents à une personne coexistent dans des endroits disparates (en définitive, chaque élément numérique est enregistré sur un disque dur ou sur un autre support doté de sa propre substance matérielle et situé en un lieu spécifique, même si la localisation de ce support peut changer au fil du temps, par exemple dans le cas où le dispositif est mobile). L'absence de frontières territoriales précises dans le monde numérique engendre à la fois des problèmes juridiques spécifiques et des problèmes généraux de perception, lors de la gestion de la vie privée.

Disparités spécifiques

Nécessité de faire en sorte que les données à caractère personnel des citoyens restent du ressort de l'Union européenne.

Aux termes de l'article 25 de la directive 95/46/CE sur la protection des données, le transfert vers un pays tiers de données à caractère personnel ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. Il existe des exceptions à cette disposition, dont le transfert vers des entreprises aux États-Unis qui respectent les principes de la «sphère de sécurité» (*Safe*

Harbour Principles).

Cependant, dans tous les cas de transfert qui échappent à la compétence de l'Union européenne, le niveau de protection défini comme étant adéquat ne prend pas en considération la possibilité que des agences de sécurité nationales aient accès à ces données. Il s'ensuit que toutes les données situées dans des pays tiers peuvent être collectées et analysées par ces agences, ce qui peut avoir des conséquences indésirables non seulement pour les particuliers, mais aussi pour les organisations et entreprises dont les secrets commerciaux risquent d'être divulgués.

Monde réel contre monde numérique.

Étant dépourvue de territorialité, la société de l'information ne dispose d'aucune frontière susceptible de la protéger. Dans le même temps, une multitude de ponts invisibles et incontrôlés se créent entre le monde réel et le monde numérique. Si nous disposons toujours, dans le monde réel, des outils nécessaires pour gérer notre vie privée (du fait des distances), tel n'est pas encore le cas dans le monde numérique. Or, ce nouvel environnement commence à faire partie intégrante de notre vie de tous les jours, du fait du nombre croissant de ponts entre ces deux univers.

Pour comprendre ce qui différencie la sphère privée de la sphère publique ou ce qui est socialement admis comme étant de la sphère privée et de la sphère publique, nous disposons de dispositions juridiques, de normes socioculturelles tacites et même de traditions. Bien que la distinction entre ces deux sphères ne soit pas toujours très nette, chacun sait qu'il existe des frontières entre elles et agit en conséquence (que ce soit, par exemple, en clôturant son terrain privé, en apposant un panneau «Défense d'entrer» sur sa pelouse, en interrogeant ou en jetant un regard mécontent à des étrangers dans un bar du quartier).

Percevoir l'espace dans le cyberespace.

Bien que les gens aient un sens intuitif de la violation de la vie privée dans le monde réel, ils n'ont pas cette même perception dans le cyberespace. Prenons un exemple: si quelqu'un est surpris à écouter une conversation, même dans un lieu public, cela sera clairement considéré comme une atteinte à la vie privée. Dans le cyberespace, il n'est pas aisé de déterminer s'il y a ou non une écoute secrète, ni même s'il s'agit là d'une violation de la vie privée. La question consiste donc à savoir comment dresser, dans le cyberespace, des barrières plus explicites entre la sphère privée et la sphère publique.

Le stockage à distance des données rend la notion de «frontières spatiales» très complexe dans le cyberespace.

Dans ce contexte et sans vouloir sous-estimer la nature déjà complexe de la «vie privée» dans le monde réel et la difficulté à la protéger adéquatement, il semble qu'il soit infiniment plus facile de violer la vie privée dans le monde numérique et infiniment plus difficile de la protéger, dans la mesure où il ne suffit pas de dédaigner une touche indésirable. De surcroît, la probabilité que les paramètres par défaut soient préjudiciables à la vie privée est plus grande dans le cyberespace, impliquant donc une vigilance permanente de la part de l'utilisateur et une action appropriée. Imaginez par exemple que, lorsque vous installez un programme ou souscrivez à un service internet en ligne, vous êtes

automatiquement abonné à des services et bulletins d'information et vous êtes informé par la suite que, si vous souhaitez vous désabonner, vous devriez vous rendre sur le site web correspondant et introduire une demande de désabonnement. Prenons un autre exemple: si vous conservez un album de photographies dans un placard de votre salon, celui-ci n'est supposé être vu que par les membres de votre famille et par vos amis et connaissances, alors qu'un album photo numérique ne jouit pas, en général, de la même protection, dès lors qu'il est possible de visualiser, voire de rechercher les photos sur l'internet[24].

La plupart du temps, l'utilisateur peut plus difficilement exercer son droit de refus et s'opposer à ces applications: il devra fournir davantage d'efforts pour y parvenir, mais aussi avoir les connaissances techniques requises. Pour compliquer encore les choses, il n'est pas rare que l'utilisateur n'ait nullement conscience du volume et du type d'informations saisies (ex.: adresses IP, *cookies*, web-tracking [localisation sur l'internet], mémoire cache, termes de recherche, etc.) lorsqu'il surfe sur l'internet ou effectue d'autres opérations en ligne. Il lui est donc d'autant plus difficile de s'opposer à la saisie de ces informations ou de protéger sa vie privée.

Des mondes virtuels.

Les mondes dits «virtuels» sont, eux aussi, exemplatifs du manque de clarté souligné ci-dessus. Certains prédisent que les entreprises les plus influentes exploiteront bientôt ces mondes virtuels. De plus, la convergence entre les réseaux sociaux et les mondes virtuels donne naissance à des applications telles que Kaneva, qui soulèvent de nombreuses questions — non encore examinées — en matière de respect de la vie privée. Quel est, par exemple, le statut juridique des données financières virtuelles (comme celles des comptes LindenDollar, par exemple)? Une autre question intéressante à se poser est la suivante: quel sens y aurait-il à délivrer une carte d'identité à un avatar? Le fait est que même une personne purement numérique peut bénéficier d'une solide authentification, associée à un contrôle de la corrélabilité des données d'identification. En tant que métaphore d'une identité numérique partielle, l'avatar peut aussi constituer une interface utilisateur protégeant utilement la vie privée.

[24] Un exemple flagrant est fourni par les services dits de «socialisation en ligne» ou «réseautage social en ligne» (tels que mySpace.com, Flickr, YouTube et Facebook) dont la configuration laisse à désirer. Ces services permettent de stocker, d'échanger, mais aussi et surtout de rechercher des photographies et des films vidéo.

Solutions proposées

Défis en matière de R&D

Faire en sorte que les infrastructures et le stockage des données n'échappent pas à la compétence de l'Union européenne.

Pour protéger les données à caractère personnel des citoyens européens, il convient, dans toute la mesure du possible, d'utiliser des mécanismes qui permettent à ces données de rester sous la compétence de l'Union européenne. Cet objectif pourrait être atteint en proposant, pour les moteurs de recherche présents sur l'internet, des serveurs proxy (ou «serveurs mandataires») pour les services extérieurs ou en mettant à disposition des moteurs de recherche distincts.

De même, il y a lieu de veiller à ce que les infrastructures d'importance cruciale restent du ressort exclusif de l'Union européenne et d'éviter toutes dépendances de la part d'autres États non membres.

Défis juridiques

La législation européenne sur la protection des données devrait être applicable à toute opération de traitement des données effectuée dans le cadre de services européens. Cette exigence permettrait d'éviter que des données ne soient inutilement stockées et exploitées.

Le concept du «territoire numérique».

En digitalisant le domaine personnel de même que ses limites, le concept du «territoire numérique» offre la possibilité d'introduire les notions de «territoire», de «propriété» et d'«espace» dans un environnement numérique. L'objectif visé est de fournir un outil qui permette aux utilisateurs de gérer la proximité qu'ils souhaitent avoir avec d'autres utilisateurs ou, au contraire, la distance qu'ils veulent garder par rapport à eux dans ce futur environnement à intelligence ambiante, tant sur le plan juridique que social, exactement comme nous le faisons actuellement dans le monde réel.

Le concept matériel et traditionnel du «domicile» fait de ce dernier un refuge légal qui protège le citoyen des interférences extérieures ou des tentatives d'intrusion dans sa vie privée[25]. Ce refuge légal doit être maintenant étendu à la partie numérique de notre sphère privée.

Défis en matière de communication

Il convient d'élaborer des outils de communication afin de préciser quels sont les éléments qui appartiennent à la sphère privée.

[25] Voir les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Liens

Beslay, L., et Hakala, H., *Digital Territory: Bubbles*, In: Paul T. Kidd (Ed.): European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society, Cheshire Henbury, 2007, p. 69 à 78.

Benoliel, D., *Law, Geography, and Cyberspace: The Case of online Territorial Privacy*, CFP 2004[26].

Daskala, B., et Maghiros, I., *Digital Territories, Towards the protection of public and private space in a digital and Ambient Intelligence environment*[27].

[26] Voir http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf.
[27] Voir http://ftp.jrc.es/eur22765en.pdf.