Défis pour la vie privée et la protection des données posés par la technologie : rapport pour l'Assemblée parlementaire du Conseil de l'Europe

Colin, Jean-Noël; de Terwangne , Cécile

Publication date:
2011

Document Version
le PDF de l'éditeur

Facultés Universitaires Notre-Dame de la Paix
Rue de Bruxelles, 61
B-5000 Namur (Belgique)
E-Mail: cecile.deterwangne@fundp.ac.be,
jean-noel.colin@fundp.ac.be
Web: http://www.fundp.ac.be

Défis pour la vie privée et la protection des données posés par la technologie

Rapport rédigé par
Cécile de Terwangne, professeur à la Faculté de Droit
Jean-Noël Colin, professeur à la Faculté d'Informatique
Université de Namur (FUNDP), Belgique

Février 2011

'The current era is one of near-exponential growth in the creation, dissemination, use and retention of personally identifiable information'

Ann Cavoukian

Information & Privacy Commissioner

Ontario, Canada

1. Introduction – Notions

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

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

Cette réalité met en cause le droit au respect de la vie privée ainsi que le droit à la protection des données.

La **vie privée**, dans ce contexte, ne doit pas se comprendre de façon traditionnelle comme une sphère intime à protéger, contenant un ensemble d'informations privées, voire confidentielles, que l'on souhaite garder cachées. Elle est à entendre comme faculté d'autodétermination, d'autonomie, capacité de l'individu à effectuer des choix existentiels[1]. En la matière, il s'agit plus précisément d'**autodétermination informationnelle**, c'est-à-dire du droit pour l'individu de « savoir ce qui se sait sur lui », de connaître les données le concernant qui sont détenues, d'en maîtriser les circuits de communication, d'en contrecarrer les utilisations abusives. La vie privée ne se réduit donc pas à une quête de confidentialité, c'est la **maîtrise** par chacun de son image informationnelle.

---

[1] Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voy. Cour eur. D.H., *Evans c. Royaume-Uni*, arrêt du 7 mars 2006, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; *Tysiac c. Pologne*, arrêt du 20 mars 2007, req. n° 5410/03 ; *Daroczy c. Hongrie*, arrêt du 1er juillet 2008, req. n° 44378/05.

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

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

a. Textes juridiques

Les textes juridiques contraignants adoptés au niveau du Conseil de l'Europe sont les premiers présentés ci-dessous. Ensuite, on mentionne le Pacte international relatifs aux Droits Civils et Politiques en tant que seul instrument universel contraignant en matière de vie privée. Enfin, ce sont les textes existant au niveau de l'Union européenne qui sont relevés.

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

L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales garantit à chacun le droit au respect de sa vie privée et familiale. Des exceptions à ce droit sont admises pourvu qu'elles soient prévues par la loi et qu'elles soient nécessaires dans une société démocratique (càd respectent le principe de proportionnalité tel que précisé par la jurisprudence de la Cour européenne des droits de l'homme – Cour EDH) pour sauvegarder les intérêts légitimes figurant dans la liste de l'article 8, § 2.

La Cour EDH a expressément élargi le champ de la vie privée à celui de la protection des données. Elle a ainsi signalé que la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée consacré par l'article 8. Pour la Cour, l'article 8 impose que le droit interne ménage des garanties appropriées pour empêcher toute utilisation impropre et abusive de données à caractère personnel. La législation nationale doit également assurer que les données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles ne sont conservées sous une forme permettant l'identification des personnes que pendant la durée nécessaire aux finalités pour lesquelles elles sont enregistrées.[2]

ii. Convention 108 du Conseil de l'Europe

Née du souci de renforcer la protection de la vie privée et des autres droits de l'individu face aux développements informatiques, la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été adoptée le 28 janvier 1981.

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

- principe de loyauté et licéité de la collecte
- principe de finalité (données enregistrées pour des finalités déterminées et légitimes et pas utilisées de manière incompatible avec ces finalités)
- principe de qualité des données (pertinentes, adéquates, à jour, conservées pour une durée limitée)
- régime spécifique réservé aux données sensibles

---

[2] Cour eur. D.H., *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, req. n° 30562/04 et 30566/04, § 103 ; également *Rotaru c. Roumanie*, arrêt du 4.5.2000, req. n° 28341/95, § 55 ; *M.S. c. Suède* arrêt du 27 aout 1997.

- exigence de sécurité
- droits d'accès, de rectification et de recours
- possibilité de dérogations au nom d'intérêts publics ou privés prépondérants

La Convention 108 a été complétée en 2001 par un Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données.

iii. Convention de Budapest sur la cybercriminalité

La Convention sur la Cybercriminalité du 23 novembre 2001 a été conçue dans le cadre du Conseil de l'Europe (STE 185) mais elle est ouverte à la signature de tout Etat dans le monde[3].

Elle impose aux Etats signataires d'ériger en infraction pénale le fait de porter atteinte à la confidentialité des données, via l'accès non autorisé ou l'interception illégale de données, ou le fait de porter atteinte à l'intégrité des données, en les altérant ou supprimant, ou à l'intégrité du système. Les Etats Parties doivent aussi sanctionner pénalement les faux informatiques et les fraudes informatiques, pour lutter contre les manipulations de données malintentionnées.

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

iv. Article 17 du Pacte international relatif aux Droits civils et politiques

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

Cette disposition est la seule disposition contraignante qui protège la vie privée à un niveau universel.

v. Charte des droits fondamentaux de l'Union européenne

Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte des droits fondamentaux de l'Union européenne[4] est juridiquement contraignante. Si l'article 7 de ce texte consacre classiquement la protection du droit au respect de la vie privée, l'article 8 présente l'originalité de garantir au sein d'un catalogue général de droits fondamentaux un droit autonome à la protection des données à caractère personnel. Cet article 8 dispose que toute personne a droit à la protection des données à caractère personnel la concernant ; que les données doivent être traitées loyalement, à des fins déterminées, sur la base d'un fondement légitime (consentement ou autre fondement prévu par la loi) ; et que toute personne a un droit d'accès et de rectification de ses données. Le respect de ces principes doit être soumis au contrôle d'une autorité indépendante.

vi. Directive européenne sur la protection des données

La directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[5] a repris, en les détaillant et les précisant, les principes contenus dans la Convention 108. Elle présente toutefois un régime

---

[3] Elle a ainsi été signée par les Etats-Unis (et ratifiée), le Canada, le Japon et l'Afrique du Sud.
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:FR:PDF
[5] *J.O.U.E.*, L 281 du 23 novembre 1995, p. 31-50.

de protection enrichi sur plus d'un point. Elle a établi une liste des seuls cas dans lesquels le traitement des données est légitime. Le catalogue des droits reconnus à la personne concernée est étoffé. Le droit d'accès englobe le droit de connaître l'origine des données et la logique qui sous-tend le traitement des données. Le droit de s'opposer au traitement de ses données et le droit de ne pas être soumis à une décision entièrement automatisée sont consacrés. En outre, un devoir d'information est mis à charge du responsable du traitement des données. Le régime des flux transfrontières qui a, lui, inspiré le Protocole additionnel à la Convention 108 est particulièrement élaboré.

vii. Directive européenne vie privée et communications électroniques

La directive 2002/58 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[6] est une directive spécifique qui s'ajoute à la directive générale (95/46) pour réglementer la protection des données dans le secteur des communications électroniques. Elle proclame l'obligation de confidentialité des communications électroniques ainsi que des données de trafic et des données de localisation, moyennant certaines exceptions. Elle instaure un devoir de sécurité des données, allant désormais de pair avec l'obligation d'informer des « violations de données » graves survenues. Cette obligation ne pèse cependant que sur les fournisseurs de services de communications électroniques accessibles au public. Ce texte règle aussi le recours aux *cookies* et l'envoi de communications non sollicitées (*spam*).

b. Textes politiques

i. Recommandation du Comité des Ministres du Conseil de l'Europe (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

Adoptée le 23 novembre 2010, cette recommandation suggère un encadrement du phénomène très répandu du profilage (v. *infra*, point 3.b.). L'annexe à la recommandation contient les principes devant conduire à un profilage loyal et licite. Une liste des cas dans lesquels le profilage est licite est établie. Le responsable est tenu de limiter les risques d'erreurs, d'adopter des mesures de sécurité et d'informer les personnes concernées de ses activités de profilage. Sauf exceptions, les individus ont le droit d'accéder aux données, de les corriger, de connaître le but du profilage ainsi que la logique utilisée pour leur attribuer un profil, et enfin, de s'opposer à l'utilisation de leurs données ou à une décision prise sur la seule base du profilage.

ii. Recommandation du Comité des Ministres du Conseil de l'Europe (99) 5 sur la protection de la vie privée sur Internet

Cette recommandation s'adresse aux utilisateurs et aux fournisseurs de services sur Internet. Elle contient des *Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes »,* destinées à être intégrées dans des codes de conduite. Ces lignes directrices énoncent les principes d'une conduite loyale à observer en matière de protection de la vie privée et des données lors des communications et échanges sur Internet.

iii. Résolution de l'Assemblée parlementaire du Conseil de l'Europe 1165 (1998) sur le droit au respect de la vie privée

Le droit au respect de la vie privée avait été défini par l'Assemblée parlementaire en 1970 dans la *Déclaration sur les moyens de communication de masse et les droits de l'homme* contenue dans sa

[6] *J.O.U.E.*, L 201 du 31 juillet 2002, p. 37-47.

Résolution 428 (1970) comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ». Près de trente ans plus tard, l'Assemblée a précisé que « *Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition le droit de contrôler ses propres données* ».

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

iv. Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et des flux transfrontières de données à caractère personnel

Premier texte apparu au niveau international en matière de protection des données, ces Lignes directrices[7] contiennent ce que l'on appelle les « Fair information principles ». Ces principes de base de la protection des données sont presque identiques à ceux contenus dans la Convention 108. A la différence de ces derniers, ils ne sont pas juridiquement contraignants.

v. La résolution de Madrid sur des normes internationales de vie privée

La Résolution de Madrid[8] de 2009 est issue d'un travail conjoint des autorités de protection des données de cinquante pays sous la houlette de l'Agence espagnole de la protection des données. Elle vise à offrir un modèle reprenant les standards universels de la protection des données. Elle réalise donc l'intégration des valeurs et principes de protection des données garantis sur les cinq continents.

Outre les aspects classiques de la protection des données, ce texte contient des éléments nouveaux comme l'invitation à prendre des mesures proactives (mesures visant à prévenir et détecter les failles de sécurité, désignation d'un correspondant à la protection des données, réalisation d'études d'impact pour la vie privée,…) et l'« Accountability principle » qui prévoit l'obligation de mettre en place des mécanismes internes permettant de démontrer que le responsable s'est conformé aux règles de protection.

vi. Résolution n° 3 des Ministres européens de la Justice sur la protection des données et la vie privée au troisième millénaire

Par ce texte, adopté le 26 novembre 2010 lors de la 30° Conférence du Conseil de l'Europe des Ministres de la Justice, ceux-ci marquent leur soutien à la modernisation de la Convention 108 afin de trouver les solutions pour garantir la protection des droits de l'individu face aux nouveaux défis de la technologie et de la globalisation de l'information. Cette modernisation devrait répondre aux préoccupations exprimées par les ministres sur les questions de transparence, d'exercice effectif des droits, de violation de la sécurité des données, de compétence territoriale et de droit applicable en présence de relations virtuelles et transfrontières (dans le *cloud computing* et les réseaux sociaux, par exemple), et de responsabilité. Les ministres signalent que la Convention 108 est à ce jour le seul instrument juridiquement contraignant de portée potentiellement universelle en la matière. Ce texte pourrait donc devenir l'instrument universel

---

[7] http://www.oecd.org/document/18/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html

[8] Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.

réclamé par les autorités nationales de protection des données. Les ministres invitent en conséquence les acteurs tiers au Conseil de l'Europe à participer au processus de modernisation.

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

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

Dans cette section, nous passons en revue une série de technologies émergentes ou en mutation, en décrivant d'une manière générale leurs applications et leur fonctionnement, mais aussi les menaces potentielles qu'elles présentent pour la vie privée et la protection des données.

a. Convergence des moyens de communication

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

Ainsi, le téléphone, doté d'une puissance de calcul et de stockage, devient par là 'intelligent' (*smart phones*) ; l'ordinateur permet de téléphoner ; la vidéo-conférence est disponible sur des baladeurs mp3 ; un numéro de fax est en fait une façade pour un email ; les appels vers un gsm peuvent être redirigés vers un poste fixe, avant d'échouer sur la boite vocale d'un service de type VOIP (Voice Over IP – téléphonie sur réseau IP) consultée sur un PC. Ces exemples montrent à quel point il devient très compliqué pour un utilisateur de déterminer le type de moyen de communication utilisé, et surtout où vont et d'où proviennent les informations envoyées ou reçues.

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

b. Géolocalisation

Des moyens de plus en plus sophistiqués et précis permettent d'établir la position géographique d'un utilisateur, que ce soit directement d'après des informations obtenues par son terminal (au moyen d'une puce GPS, de plus en plus répandue dans les téléphones portables) ou via le réseau auquel il est connecté

(par triangulation des bornes GSM, ou l'utilisation de bases de données reprenant la localisation des réseaux wi-fi – voir à ce sujet les informations collectées par la *Google Car*[9]).

La gestion des transports publics de manière électronique permet aussi de suivre les déplacements des usagers, par exemple à partir de la validation de leur titre de transport auprès de bornes.

La position de l'utilisateur est parfois conservée ou communiquée à des tiers sans informer ni obtenir son consentement, avec pour conséquence un traçage possible des déplacements, un profilage des absences du domicile… Cela met en cause la liberté de circuler anonymement.

De façon encore plus pernicieuse, l'information de géolocalisation lors de la prise de photos (avec un téléphone portable par exemple), combinée aux technologies de reconnaissance faciale, telles qu'implémentées entre autres dans les logiciels Apple iPhoto® ou Google Picasa®, permettent de déterminer la localisation d'une personne figurant sur une photo, à son insu.

c. Traçabilité des utilisateurs

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

d. Adressage IPv6

En raison de la prolifération des systèmes connectés à Internet, la plage d'adresses définie par la norme IPv4[10] est épuisée, ce qui menace l'expansion d'internet. En réponse à ce problème, la norme IPv6 a été créée, qui supporte un nombre beaucoup plus important d'adresses distinctes[11]. A titre d'illustration, IPv6 permettrait à chaque individu sur terre de disposer de plusieurs dizaines de milliards de milliards de milliards d'adresses pour son usage personnel.

L'assignation d'une adresse IPv6 à un équipement peut être réalisée de différentes manières, dont l'une utilise l'adresse physique (adresse MAC) de l'appareil pour générer l'adresse IPv6, ce qui permet alors de lier le trafic à une machine, voire de conduire à une personne. D'autres modes permettent d'éviter cette situation, en générant des adresses de manière pseudo-aléatoire ou en recourant à un serveur d'adresses qui les assigne de manière automatique[12].

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

---

[9] Voir à ce sujet http://pro.clubic.com/entreprises/google/actualite-343282-google-acces-wi-fi-repertories-grande-bretagne.html ou http://www.infos-du-net.com/actualite/17071-google-wi-fi-reseaux.html

[10] IPv4 définit un format d'adresse sur 4 bytes, représentant chacun une valeur entre 0 et 255, soit $2^{32} \simeq 4.10^9$ adresses possibles

[11] IPv6 utilise un format d'adresse sur 16 bytes, représentant chacun une valeur entre 0 et 255, soit $2^{128} \simeq 256.10^{36}$ adresses distinctes

[12] Ce mécanisme utilise le protocole DHCP

e. Cookies

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

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

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

f. Réseaux de distribution intelligents

L'on assiste à une évolution des réseaux de distribution d'énergie vers une forme intelligente (Smart Grid) dans laquelle sont incorporées des technologies informatiques afin d'optimiser la production et la distribution, l'objectif étant d'ajuster au mieux la production et la consommation, conduisant ainsi à des économies d'énergie, l'évitement de pannes… Le Smart Grid fonctionne à partir de compteurs intelligents, munis de capteurs et reliés via un réseau à un système qui collecte, intègre et analyse les données de consommation.

Les compteurs intelligents communiquent les informations de consommation en temps réel à l'opérateur, ce qui peut constituer un moyen de profiler les consommateurs : absence ou présence dans le bâtiment, utilisation d'appareils possédant une 'signature' énergétique…

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

Dans ce cas encore, l'on assiste à une collecte massive d'information pouvant être liée à une personne ou un groupe de personnes, permettant d'en déduire des caractéristiques et des comportements de manière très ciblée. Lorsqu'en plus cette information est collectée par des tiers, comme c'est le cas pour le système PowerMeter[13] de Google, le risque de diffusion non contrôlée de l'information est encore plus grand.

g. RFID et l'Internet des Objets

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

- L'étiquette, ou tag, qui est collée ou intégrée à l'entité à identifier

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

- Le lecteur, utilisé pour interroger le tag lorsque celui-ci est à sa portée
- Le système d'information, qui reçoit l'information du lecteur et la traite

Le tag est composé d'une antenne et d'une puce électronique, qui contient, au minimum, un identifiant. Lorsque le tag est interrogé par un lecteur (par l'utilisation d'ondes magnétiques), il transmet son identifiant au lecteur. La structure du tag est très simple, de manière à permettre une production de masse à un coût permettant son utilisation massive, typiquement quelques centimes[14]. La lecture du tag ne nécessite pas de contact entre celui-ci et le lecteur ; en fonction du type de tag, la distance de lecture peut varier entre quelques centimètres ou quelques dizaines de centimètres, voire au-delà.

Les tags RFID sont utilisés dans la gestion des stocks et de l'approvisionnement, pour les péages routiers, dans la grande distribution pour la gestion de l'inventaire, des caisses ou du service après-vente, dans les aéroports pour le suivi des bagages ou comme moyen de marquage des animaux. Dans certains cas, les tags peuvent être implantés chez des êtres humains, par exemple pour assurer la sécurité d'enfants ou de personnes âgées, ou, dans un registre plus léger, pour surveiller l'accès ou gérer les consommations dans une discothèque.

L'identifiant étant spécifique à un tag, la lecture de celui-ci permet donc de suivre ses déplacements, d'après la position du lecteur, et donc ceux de l'objet ou de la personne qui le porte. La lecture se faisant à distance, l'utilisateur n'est pas nécessairement conscient de celle-ci, ce qui peut conduire à des fuites d'information ou un traçage à son insu. L'interrogation simultanée d'un grand nombre de tags permet d'identifier très rapidement les objets ou personnes marquées dans un environnement proche, et donc là aussi aboutir à un profilage du porteur.

Différentes solutions techniques existent (et d'autres continuent d'être développées) qui permettent de limiter les possibilités d'utilisation malveillante des technologies RFID. Mais bien souvent leur mise en œuvre fait augmenter significativement le coût de fabrication, rendant difficile leur utilisation à large échelle.

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

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

[14] Notons qu'un tag peut être plus élaboré : il peut contenir plus d'informations que l'identifiant et posséder sa propre batterie, pour atteindre des distances de transmission plus élevées ou agir comme capteur, par exemple.

h. Robots d'indexation

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

Certains robots malveillants analysent les pages pour en extraire les adresses emails afin de constituer des listes de diffusion pour l'envoi de spam. D'autres peuvent aussi parcourir des pages, afin d'agréger et de corréler les informations collectées et en inférer d'autres.

i. Données biométriques

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

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

j. Privacy by Design

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

C'est Ann Cavoukian, Commissaire à l'Information et la Vie Privée de la province d'Ontario, Canada, qui est à l'origine de cette initiative, fondée autour des valeurs de respect de l'utilisateur, de transparence à son égard pour ce qui concerne la collecte et le traitement des données, et de refus de compromis dans lesquels la vie privée serait sacrifiée au profit d'autres objectifs. Les principes de base sont le caractère proactif des mesures de sécurité, le fait que par défaut, la protection des données est assurée, toute dérogation devant avoir l'approbation de la personne concernée, le fait que la protection des données doit être considérée comme partie intégrante des fonctions du système d'information, plutôt qu'une fonctionnalité annexe, et qu'elle doit être maintenue tout au long du cycle de vie de l'information collectée.

Ces principes sont applicables aussi bien au domaine IT, qu'à celui des pratiques métiers et de l'infrastructure physique.

Un portail internet est consacré à cette approche[15], qui outre une présentation générale, démontre l'applicabilité de la démarche au travers de nombreux cas d'études, montrant ainsi qu'il est possible de concevoir des systèmes efficaces et répondant aux exigences-métier sans pour autant sacrifier à la protection des données.

[15] http://www.privacybydesign.ca/

k. Cloud computing

Le 'Cloud Computing' est un paradigme récent d'architecture IT, qui rend complètement transparent pour l'utilisateur l'endroit où les données qu'il manipule et les services qu'il utilise sont effectivement stockés ou mis en œuvre. Le terme fait référence à la fois aux services accédés et délivrés via Internet, et aux systèmes d'information et à l'infrastructure matérielle et logicielle qui fournit ces services.

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

Les services de type 'Cloud' peuvent être offerts à différents niveaux ; on distingue généralement trois modèles différents :

- Infrastructure as a Service (IaaS) : les services offerts sont de type 'infrastructure', soit principalement du matériel et du logiciel de base, ainsi que de la connectivité ; la gestion de cette infrastructure est laissée au client ;
- Platform as a Service (PaaS) : les services offerts prennent la forme d'une plateforme opérationnelle, composée de l'infrastructure, mais aussi de l'environnement logiciel permettant au client de développer ou d'exploiter ses propres applicatifs ; la gestion de l'ensemble est donc partagée entre le fournisseur de service et son client ;
- Software as a Service (Saas) : le fournisseur offre ici une solution applicative complète à son client, en prenant en charge à la fois l'infrastructure, mais aussi l'application. De tels services sont offerts par exemple par salesforce.com, pour la gestion commerciale, ou par Google, au travers de ses services mail, documents, agenda…

Le 'Cloud Computing' constitue donc une extension du périmètre de sécurité vers Internet, où il est fort compliqué d'effectuer un contrôle efficace. Le stockage de ses données est confié par l'utilisateur à un tiers, le fournisseur de service, qui les héberge et les traite dans des conditions bien souvent inconnues de l'utilisateur. Ceci nécessite une réelle relation de confiance entre l'utilisateur et le fournisseur de service. Cette confiance peut être renforcée par des garanties contractuelles.

Les défis principaux se situent autour de la protection des données confiées au Cloud, de la préservation de leur intégrité et du maintien d'un contrôle d'accès approprié.

l. Deep packet inspection

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

Le filtrage du trafic réseau, opéré typiquement par des pare-feux (firewalls) se base pour autoriser ou non le transit sur les informations de routage, présentes dans l'en-tête des paquets, soit principalement l'origine et la destination du message. Le 'Deep Packet Inspection' se base en plus sur des critères de contenu, en analysant non seulement l'en-tête, mais aussi le corps du message, soit son contenu.

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

4. Défis pour la vie privée et la protection des données liés aux usages

a. Collecte et traitement d'informations recourant aux TIC

i. Par les autorités étatiques

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

Le recours aux identifiants uniques servant d'instruments d'interconnexion et d'accès transversal aux données d'un individu augmente encore les risques de perte de contrôle et de non-respect de la proportionnalité.

Les inquiétudes face aux traitements de données personnelles par les autorités publiques sont accentuées par le fait que ces traitements servent de base à la prise de décisions telles l'octroi d'une pension, la reconnaissance d'un statut particulier, l'établissement de l'impôt, l'ouverture d'enquêtes pénales,…

ii. Par les entités commerciales

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

- pour les acteurs offrant des services via Internet car connaître le profil des internautes intéressés par les produits ou services et pouvoir détailler très précisément leur intérêt (pages web lues, liens cliqués, fréquence des visites,…) permet de configurer l'offre de manière optimale ;
- pour les acteurs exploitant commercialement des bases de données nominatives : récolter des données tous azimuts permet de constituer de très riches bases de données exploitables et revendables pour des activités de marketing et de mailing ;
- pour le fonctionnement même du Web : la gratuité de la plupart des services offerts sur le Web n'est que de façade. L'exposition publicitaire des utilisateurs finance l'offre. Le modèle économique repose sur le marketing. Celui-ci sera d'autant plus rentable que le profil des destinataires est précis et permet de cibler efficacement les messages publicitaires.[16]

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

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

Cet ensemble de mots est le plus souvent incroyablement révélateur de ses centres d'intérêts, ses activités, ses projets,…

iii. Par les employeurs

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

Les TIC représentent aussi des instruments de connaissance. Bon nombre d'employeurs se renseignent à la source du Web sur les candidats employés. Google et Facebook, notamment, jouent ainsi le rôle d'indicateurs et révèlent au futur patron des facettes des candidats qui ne se trouvent pas sur leurs CV…

iv. Par les individus eux-mêmes

Dans bien des cas, les individus ne prennent pas la pleine mesure de la portée de leurs actions sur le réseau. Le Web 2.0 leur a donné la possibilité d'interagir, d'apporter des commentaires, de diffuser eux-mêmes du contenu, de partager en continu savoirs, photos, vidéos, informations, états d'âme,… Toutefois le rayonnement de l'information sur Internet dépasse parfois largement ce à quoi on s'attend. L'exemple des informations tirées des pages publiques de Facebook et jointes automatiquement, à l'insu de la personne concernée, par un logiciel de courrier électronique aux courriels envoyés a déjà été cité *supra*. La puissance des robots « ratisseurs » qui alimentent les moteurs de recherche permet de faire remonter des informations trouvées à des endroits épars, publiées dans des contextes qu'on croyait particuliers à des personnes qu'on croyait restreintes. Ce qui est émis dans un certain cercle (par exemple un commentaire déposé sur un forum de discussion) risque donc de réapparaître, sorti de son contexte et juxtaposé à d'autres informations.

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

Cette perte de contrôle est d'autant plus inquiétante qu'elle s'accompagne de l'*eternity effect.* A l'inverse de la mémoire humaine, la mémoire électronique n'efface rien si ce n'est volontaire. Des éléments peuvent remonter éternellement du passé tant qu'on n'a pas pris la décision, le temps et l'énergie de les supprimer (là où on a la maîtrise de la suppression).

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

b. Profilage des internautes

Le profilage consiste à appliquer des algorithmes à des quantités d'informations agrégées, pour mettre au jour des corrélations entre les données et faire surgir des profils. Ces derniers sont appliqués à un individu, pour décider du traitement à lui réserver (le considérer ou non comme fraudeur fiscal, ou comme cible de

marketing de tel produit, ou comme voyageur candidat terroriste,…). Motivé par un intérêt économique (cf. *supra*, point a.ii.), sécuritaire ou autre, le profilage est facilement réalisable à partir des informations disponibles à grande échelle (traces, mots introduits dans les moteurs de recherches, etc.) et du recours aux cookies, notamment.

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

c. Rétention des données

Les données liées à l'utilisation d'Internet et des nouveaux moyens de communication représentent une mine de renseignements précieux pour les activités de recherche policière et de lutte contre la criminalité.

Depuis les attentats du 11 septembre 2001, des textes ont été votés au niveau européen pour harmoniser les situations dans lesquelles des données relatives au contenu ou des données de trafic ou de localisation sont conservées pour être tenues à la disposition des autorités pénales. Ces données portent sur la durée, la date, les destinataires, le lieu de toutes les communications, le volume des SMS/textos et des courriels,….

Il est intéressant de voir la progression de ces textes. La Convention sur la cybercriminalité de novembre 2001 prévoit que les Etats peuvent imposer la conservation rapide de telles données, à la demande d'une autorité, pour des données spécifiées et pour maximum 90 jours. La directive 2006/24 du 15 mars 2006 sur la conservation de données, quant à elle, impose aux fournisseurs de services de communication (Internet, téléphone, mobiles, fax) la rétention des données de trafic et de localisation de tout le monde, de façon systématique et pour une durée entre 6 mois et deux ans…

5. Conclusions

a. Possibilité d'autorégulation par le secteur privé

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

La régulation du secteur privé ne se limite toutefois pas aux technologies mais devrait également couvrir les usages et pratiques en place dans ce secteur et évoquées ci-dessus.

Une des faiblesses de l'autorégulation c'est qu'elle repose sur l'initiative et la bonne volonté des acteurs. Il est cependant clair qu'une conscientisation collective fait inévitablement pression sur ces acteurs et que cela peut augmenter leur motivation liée à leur image ou à celle de tout un secteur d'activité. Une autre faiblesse

tient au fait qu'à la différence de la législation, l'autorégulation n'est pas le fruit d'une confrontation de points de vue devant aboutir à un équilibre. Les règles établies étant la plupart du temps issues d'une seule catégorie d'acteurs, elles ne reflètent que la prise en compte des préoccupations par ces seuls acteurs et leur perception de l'équilibre socialement et économiquement admissible.

Les mesures d'autorégulation complètent et soutiennent les règles légales. Elles renforcent très certainement leur effectivité. Elles devraient être largement encouragées mais, étant donné leurs faiblesses, ne devraient pas se substituer à l'action du législateur national ou international.

b. Lacunes des législations européennes

Les législations existantes pèchent par un manque d'effectivité et par des lacunes quant au contenu du régime de protection.

Tant la Convention 108, que les Lignes directrices de l'OCDE et la directive générale de protection des données ont été conçues avant l'avènement d'Internet. La dimension globalisée des services d'information, le contexte virtuel et transfrontière n'ont pas pu être pris en compte lors de l'élaboration du régime de protection. L'opacité terriblement généralisée du système et les pernicieuses possibilités de surveillance n'ont pu être anticipées.

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

Le respect des législations peut être amélioré notamment en renforçant les pouvoirs des autorités de contrôle et en instaurant un droit d'action collective en justice. Un mécanisme de contrôle des législations nationales préalablement à la ratification de la Convention 108 pourrait aussi être mis en place.

Cela étant, une amélioration sur le plan de l'effectivité passera en outre impérativement par une plus grande sensibilisation des usagers.