COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 18 novembre 2004 T-PD (2004) 04 final

Restreint

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL
(T-PD)

RAPPORT SUR L'APPLICATION DES PRINCIPES DE PROTECTION DES DONNEES AUX RESEAUX MONDIAUX DE TELECOMMUNICATIONS

L'autodétermination informationnelle à l'ère de l'Internet

Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD)

Par

Yves Poullet
Expert auprès de l'Unesco et de la Commission européenne
Doyen de la Faculté de droit de Namur
Directeur du Centre de Recherche Informatique et Droit

Jean-Marc Dinant, Maître en Informatique
Expert auprès de la Commission belge de protection de la vie privée et du Groupe 29
Maître de conférences et chargé d'enseignement à l'Université de Namur

Avec la collaboration de
Cécile de Terwangne, Professeur à la Faculté de Droit de l'Université de Namur
Maria Veronica Perez- Asinari, Senior Researcher au CRID

Les experts signataires de ce rapport
expriment ici leur opinion personnelle qui n'engage pas le Conseil de l'Europe

TABLE DES MATIERES

INTRODUCTION

Le rapport avait pour mission d'aider le Comité consultatif à identifier des pistes de recherche et de travaux futurs et ce dans une optique prospective. Il s'agissait de pointer quelques défis et enjeux du développement technologique des réseaux et services de communication électronique et de proposer à partir de là quelques thèmes de recherche ou objets de recommandations qui pourraient être proposées par le Comité consultatif au Conseil des Ministres ad hoc.

Dans ce contexte, le rapport se propose, à partir d'une description des modifications du « paysage technologique » depuis la date d'approbation de la Convention n° 108 et de quelques enjeux importants liés à ces modifications (Partie I) dans un premier temps, de confronter les dispositions de la convention n° 108 aux enjeux de ces réalités nouvelles (partie II) et dans un second temps de proposer les principes nouveaux de ce que la conclusion appelle la troisième génération de réglementations de la vie privée (partie III).

L'élaboration du rapport traduit des idées progressivement mûries de travaux personnels et au sein d'institutions de protection des données. Leur expression finale se fonde sur des discussions que nous avons voulu mener tout d'abord entre chercheurs de notre centre. Sur ce point, nous tenons à remercier tout d'abord Mme Cécile de Terwangne et Mme Maria Veronica Perez Asinari pour leur collaboration à l'écriture de ce rapport et les multiples discussions qui nous ont contraint sans cesse à préciser ou enrichir notre propos . D'autres collègues namurois peuvent être remerciés, ainsi Mme Karen Rosier et Mr T. Léonard. Au delà du cercle namurois, les idées ont été, dans une première version, proposées à divers cénacles, ainsi lors d'une conférence organisée par le Garante italien en juin de cette année mais surtout lors de la première réunion de présentation du rapport au Comité consultatif T|-PD ce même mois de juin et à la Conférence de Prague du mois d'octobre organisée par le Conseil de l'Europe, les 14 et 15 octobre[1]. Il est indéniable que le Rapport n'eût pu être ce qu'il est devenu sans les multiples apports reçus lors de ces différentes présentations, le nombre de réactions reçues nous a en tout cas conforté dans l'idée que nos intuitions de départ pour être partielles n'en étaient pas moins fondées.

Pour permettre au lecteur une lecture plus aisée, nous avons mis en gras et sous la rubrique : « Piste de réflexion », les domaines où une recherche plus pointue apparaît nécessaire et quelques suggestions adressées à cet égard. Ces rubriques ne sont pas systématiques. Semblablement, pour la même raison, nous n'avons pas voulu encombrer le lecteur de notes de bas de pages, renvoyant sur ce point aux quelques articles ou ouvrages doctrinaux cités de même qu'à certains documents. Nous ne prétendons pas avoir été exhaustifs, nous n'affirmons pas que les questions pointées soient les seules importantes au regard du thème que nous avions à analyser, nous avons cherché simplement et à partir des points de vue qui étaient les nôtres à énoncer et articuler quelques opinions en espérant qu'elles puissent être partagées.

---

[1] Cf. Y. POULLET, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », rapport à paraître dans les Actes de la Conférence. Certains éléments de ce rapport ont été repris dans le présent document (Cf. en particulier , la partie III)

LA NOUVELLE VULNERABILITE DE L'INDIVIDU FACE A L'EVOLUTION DES RESEAUX MONDIAUX DE TELECOMMUNICATION : PAYSAGE TECHNOLOGIQUE ET ACTEURS.

1. Introduction

L'objet de cette première partie consiste à évaluer les risques concrets[2] et habituels[3] courus par la personne individuelle dans sa vie privée ou professionnelle et liés à son utilisation des réseaux électroniques de télécommunication. Le présent rapport ne s'attache donc pas à l'analyse des risques liés à la gestion de dossiers purement manuels ou à la transmission d'informations sur un support physique autre qu'un terminal de télécommunication.

Un problème généré par le développement de ces réseaux est le déséquilibre informationnel qui a été créé entre les responsables de traitements et les personnes concernées, entre les « ficheurs » et les « fichés ». La technologie ambiante, qui se base sur des ordinateurs de plus en plus rapides, puissants, miniaturisés et omniprésents, possède cette propriété de collecter et transmettre, en pratique et systématiquement, de nombreuses traces tout en laissant dans l'ombre l'existence, la nature ou la finalité de cette collecte.

La réponse à cette première partie pourrait être une question : « comment se protéger ?». La question nous semble bien mal posée. Elle présuppose que c'est à l'individu et à lui seul qu'incombe la tâche de se protéger. La question préliminaire consiste à se demander « qui va protéger ? ». De cette question surgit bien évidemment, de manière implicite mais certaine, la question du financement et de la responsabilité de cette protection.

2. Le paysage technologique et son évolution.

2.1. LA SITUATION EN 1980

Il faut se rappeler, qu'il y a à peine une génération, l'Internet, tel qu'il existe maintenant, était tout simplement inconcevable.

Pour mémoire, le premier ordinateur personnel massivement distribué apparaît au début des années 80. Il s'agit de l'IBM PC junior équipé déjà à l'époque du MicroSoft Disk Operating System (MS-DOS). Les réseaux locaux des entreprises commencent à se

---

[2] Il ne s'agit vraiment pas ici de décrire ce qui pourrait se faire mais ce qui se fait en pratique avec une vision prospective sur ce qui pourrait se faire dans un avenir proche.

[3] Le profil type qui nous intéresse est l'internaute de la rue. Un citoyen de l'internet (netizen) qui n'est pas technicien, qui n'a pas un budget ou un temps considérable à consacrer à sa protection. Il va de soi que le lecteur de ce rapport pourra objecter que dans telle ou telle situation particulière, il est possible pour l'individu de se prémunir de certains risques en adoptant telle ou telle attitude. Hormis le fait que ces attitudes supposent bien souvent un niveau d'instruction, une compétence technologique, un temps voire un budget non négligeables, ce que nous excluons par hypothèse, la réponse à ce type d'argument consiste à y opposer l'analyse de la genèse du risque : n'y avait-il pas moyen de concevoir une autre technologie pour que l'internaute ne doive pas avoir à se protéger ? Un des dangers majeurs qui guette la société des réseaux de télécommunication est d'aboutir à une marginalisation, une pénalisation voire une exclusion, des personnes soucieuses de protéger leur anonymat (y compris leur non traçabilité).

développer dès 1985. Le réseau téléphonique RNIS[4] (dénommé Numéris en France) se développera vers 1987. Le premier « browser » apparaît en 1990-91 et permettait de « surfer » sur un nombre très réduit de sites, principalement américains. A cette époque, la vitesse des lignes privées était de l'ordre de 2400 à 9600 bits par seconde. Les téléphones mobiles apparaissent vers le milieu des années 1990.

Avant 1990, pour la plupart des gens, les réseaux de télécommunication se résumaient à deux usages : le téléphone, voire le téléfax. De nombreux usages n'étaient pas liés à l'utilisation d'un réseau de télécommunication téléphonique : et notamment : lire un journal, commander un bien ou un service, écouter la radio, regarder la télévision, placer une petite annonce, consulter un annuaire ou des petites annonces, effectuer un paiement, ouvrir une porte, envoyer ou recevoir du courrier, etc.

2.2. LA NUMERISATION DE L'INFORMATION ET DE SA TRANSMISSION

Le premier changement fondamental lié au développement des NTIC est la digitalisation des signaux sonores, visuels et de l'information elle-même. Actuellement, tout contenu audible ou visible est numérisable, c'est à dire peut être transcrit sous forme de « 0 » ou de « 1 » et donc stocké et transmis par des équipements électroniques. Cette numérisation s'est déployée au niveau mondial grâce à des algorithmes de numérisation internationalement standardisés (par exemple JPEG pour les photos, EFR pour la voix, MPEG pour les images en mouvement, etc.) connus de tous et qui détaillent les règles universelles permettant de passer d'un contenu analogique à un contenu binaire et vice-versa. Les téléphones modernes (ISDN ou GSM) ont pour caractéristiques de numériser la voix en temps réel, de l'envoyer sur le réseau sous forme binaire et, à l'arrivée de transformer l'information ainsi digitalisée en un signal vocal audible.

On peut se demander quel est l'intérêt de procéder systématiquement à la numérisation de tout signal. Cet intérêt est double. D'une part, il permet à des ordinateurs de plus en plus petits et puissants de traiter ce signal. Par ailleurs un autre phénomène vient s'inscrire à la suite du premier : il s'agit de la « paquétisation ».

Les réseaux téléphoniques d'antan fonctionnaient sur base d'une **commutation de circuits**. Cela signifie que chaque central téléphonique était, en fait, une centrale d'aiguillage qui avait pour effet de connecter physiquement entre eux certains fils de manière à laisser passer le courant électrique véhiculant un signal analogique représentant la voix. Cette manière de faire n'est pas optimale pour plusieurs raisons. Il y a nécessité de créer un lien physique de bout en bout entre deux personnes, parfois sur de longues distances et ce faisant chaque portion de la ligne utilisée par deux personnes est rendue inutilisable pour les autres. Ce point s'avérait d'autant plus gênant que la capacité de transmission d'un seul canal allait en augmentant. Pour pallier cet inconvénient, on a utilisé des systèmes de multiplexage en temps ou en fréquence permettant de créer plusieurs canaux de communication virtuel sur un même support physique.

A l'heure actuelle, sur Internet et sur les autres réseaux, la commutation qui s'opère est, en règle générale, une **commutation par paquets** et non plus par circuit. L'information, préalablement numérisée, est envoyée sous forme de nombreux paquets de petite taille

---

[4] Pour Réseau Numérique à Intégration de Service (an anglais Integrated Services Digital Network) : réseau téléphonique entièrement digitalisé.

(typiquement de quelques dizaines de bits à quelques centaines). En fait, la commutation par paquet permet en général une utilisation optimale de la bande passante et donc de la capacité du support de télécommunication. Cette manière de faire permet un partage extrêmement souple d'un seul support de communication entre des centaines, voire des centaines de milliers, d'utilisateurs simultanés.

Chaque paquet comporte l'adresse de l'expéditeur et l'adresse du destinataire. Sur le réseau, chaque nœud (aiguillage) qui reçoit un paquet sait sur quelle voie envoyer ce paquet sur base de son adresse de destination (on appelle cela le routage). Si, pour une raison ou pour une autre, il ne sait pas envoyer ce paquet, il peut le renvoyer au nœud qui lui a envoyé ce paquet avec une explication.

Une conséquence importante est, en ce qui nous concerne, que le destinataire connaît ou peut connaître le point d'expédition voire l'adresse de l'expéditeur, puisque celle-ci figure sur le paquet qu'il reçoit.

2.3. DES PERFORMANCES EN CROISSANCE EXPONENTIELLE POUR LES SUPPORTS DE TELECOMMUNICATIONS

Un autre élément récurrent des réseaux de télécommunication consiste en l'augmentation perpétuelle de leurs performances à de nombreux niveaux. On peut relever quelques tendances majeures .

1. **l'augmentation du débit**[5]. En l'état actuel de l'art, la fibre optique, insensible aux parasites électromagnétiques, permet des débits de l'ordre de dix giga (=milliards) bits par seconde[6]. Les câbles actuels contiennent plusieurs fibres optiques(de quelques dizaines à quelques centaines). Grâce à la technologie DSL, il est aujourd'hui classique d'atteindre des débits allant jusqu'à quatre méga (=millions) bits par seconde sans devoir modifier le fil téléphonique classique à paire torsadée enterré dans le sol et avec un appareillage de quelques dizaines d'Euros. Ceci signifie, qu'à terme, il est techniquement possible que la télévision emprunte la voie de l'Internet plutôt que celle du satellite ou de la télédistribution par câble coaxial dédicacé. Des expériences en ce sens sont d'ailleurs en cours dans de nombreux pays. Ceci présente un nouvel enjeu. Actuellement le satellite et le câble de télédistribution, techniquement, ne permettent pas ou peu à l'émetteur de programme de savoir quels sont les programmes regardés par l'abonné (techniquement, tous les signaux arrivent sur l'équipement terminal[7] de l'abonné et c'est celui-ci qui choisit celui qu'il veut regarder). Avec la télévision sur Internet, il sera possible de savoir sur une base individuelle qui regarde quoi et même d'injecter de manière ciblée des publicités à des moments précis, toujours sur une base individuelle.

2. **L'évolution de la puissance de traitement.** L'évolution de cette puissance s'est déroulée de manière corrélative à la puissance et à la capacité des composants des ordinateurs. En 1987, un ordinateur personnel typique possédait un processeur à 8 méga

---

[5] Pas en termes de rapidité. La rapidité est une notion distincte de celle du débit. Grosso modo, l'information sur un fil de cuivre ou dans une fibre optique circule toujours à la vitesse de la lumière. L'augmentation du débit relève d'une capacité à alterner plus rapidement les « zéros » et les « uns »

[6] Il s'agit de ce qui est installé actuellement. Des prototypes permettent d'aller beaucoup plus vite.

[7] C'est pour cela qu'il est possible d'enregistrer un programme de télévision tout en en regardant un autre simultanément.

hertz avec 640 KB de mémoire vive et un disque dur de 20 méga bytes. A l'heure actuelle, en 2004, le standard en vente dans les supermarchés possède un processeur de 2,4 giga hertz (performance multipliée par 3000), 256 MB de mémoire vive (400 fois plus) et un disque dur de 60 Giga bytes (3.000 fois plus). A vitesse égale, les processeurs modernes sont en outre nettement plus puissants que leurs prédécesseurs et le nombre de processeurs présents au sein d'un ordinateur a tendance à se multiplier, certains d'entre eux devenant spécialisés (ASIC[8]) et gérant une tâche bien particulière (par exemple, l'affichage ou l'envoi et la réception de signaux sur le réseau,…). Certains traitements, qui étaient jadis impossibles autrefois, deviennent aujourd'hui réalité. L'échantillonnage et la numérisation d'une voix ou d'une image peuvent aujourd'hui s'opérer en temps réel tout en offrant une qualité très proche de l'original.

3. **La polyvalence des réseaux de télécommunication**. Cette polyvalence est permise par la digitalisation de tous les types de contenus (texte, image, vidéo, voix, etc.) qui permet leur représentation universelle sous forme de bits. Par ailleurs, les augmentations substantielles du débit permettent la transmission en temps réel de contenus riches et complexes comme le multimédia.

4. **Connectivité permanente**. Celle-ci constitue un autre trait marquant de l'évolution des télécommunications ces dernières années. Cette caractéristique est permise par l'augmentation des débits ainsi que la circulation de l'information par paquets. En outre la progression des réseaux sans fil permet la mobilité des terminaux de télécommunication et leur connectivité durant le déplacement

5. **La tarification forfaitaire** Dans de nombreux réseaux, la tarification se compose d'un abonnement qui représente la connexion au réseau et éventuellement un coût supplémentaire marginal pour certaines utilisations du réseau. L'impact de cette tarification est double. D'une part, dans le cadre d'une tarification forfaitaire, l'opérateur du réseau n'a plus de raison de collecter et de conserver des données de trafic puisqu'il ne facture plus chacune des communications. D'autre part, la tarification n'est plus orientée sur les coûts, en tout cas plus sur une base individuelle. Une tarification « à l'acte » posera toujours plus de problème pour le respect de la vie privée qu'une tarification forfaitaire.

6. **La pseudo gratuité** Il est classique aujourd'hui que les individus voulant bénéficier d'un service de la société de l'information (par exemple envoyer un email, surfer sur la toile, etc.) se voient offrir, si pas le terminal, au moins le logiciel permettant d'accéder à ce service. Or, en pratique, ces logiciels « client » sont nettement plus nombreux et plus complexes à produire et à maintenir que les logiciels serveurs correspondants. En d'autres termes, lorsque Microsoft vend son serveur HTTP Internet Information Server ASP, il vend aussi, quelque part, le service qui consiste à offrir gratuitement à des dizaines de millions d'utilisateurs le browser (MSIE) qui permet de se connecter sur ce serveur. Cette gratuité n'est donc pas orientée sur les coûts, loin s'en faut, mais provoque des distorsions de la concurrence pour des firmes qui souhaitent produire uniquement des logiciels « client » (comme Opéra ou

---

[8] Application Specific Integrated Circuit : Processeur spécialement conçu pour une tâche particulière (p.e. la digitalisation d'un signal analogique, le (dé)chiffrement,…). Typiquement, une puce ASIC ira environ cent fois plus vite qu'un processeur non dédicacé pour accomplir une tâche spécialisée.

Mozilla). Sans rentrer dans les détails[9], ces derniers venus sur le marché proposent pourtant des fonctionnalités nettement plus protectrices de la vie privée.

La plupart des équipements des réseaux peuvent aujourd'hui fonctionnellement être définis comme des ordinateurs et il y a lieu de rappeler ici la loi de Moore qui établit que la performance de ceux-ci double tous les dix-huit mois, ou encore est multipliée par mille tous les quinze ans et que le prix diminue de moitié à performance égale. Cela signifie que, toutes autres choses égales par ailleurs, la puissance des ordinateurs sera multipliée par mille en 2019. De nombreux experts prédisent toutefois que cette loi aura un terme lorsque la taille des circuits atteindra la dizaine de nanomètres. Toutefois, parallèlement, il est possible, qu'à terme, l'optronique[10] replace l'électronique et permette ainsi un saut de performance fabuleux.

Face à cela, il convient de souligner que les capacités sensorielles de l'être humain n'ont pas sensiblement évolué durant cette période. Le débit binaire nécessaire pour un son se situe toujours entre 10kbits/seconde (voix) et 20kbits/seconde (haute fidélité) et un film avec le son nécessite entre 256kbits/seconde (vidéoconférence) et 2 gigabits pour la haute qualité.

En conclusion, il est devenu et il deviendra de plus en plus possible et de moins en moins cher d'enregistrer la vie de tous les individus de la planète (la nôtre et celle des autres…).

A titre d'illustration, nous pouvons examiner la faisabilité de l'enregistrement de *toutes* les communications téléphoniques sortant d'Europe vers le monde entier. Ce n'est pas rien puisqu'il s'agit de stocker l'équivalent de cinquante milliards de minutes de télécommunication vocales[11] sur une base annuelle[12]. Si l'on considère qu'il faut environ dix mille bits par seconde pour digitaliser la voix, on observe qu'il faudra en moyenne de l'ordre de dix tera (=mille milliard) bytes pour stocker 24 heures de trafic, ce qui à l'heure actuelle est tout à fait envisageable avec des systèmes de disk array où chaque disque peut stocker de l'ordre de 400 giga bytes[13]. En outre, le débit moyen de ce flux continu de centaines de milliers de communications simultanées représente un débit moyen d'environ 10 giga bits par seconde, ce qui est supportable par une seule fibre optique de l'épaisseur d'un cheveu[14]. En d'autres termes, il serait techniquement possible de faire passer TOUT ce trafic téléphonique à travers un mince tube en verre de quelques microns d'épaisseur et de l'enregistrer à un prix raisonnable en achetant du matériel classique que l'on trouve en vente libre sur Internet.

---

[9] Signalons que Mozilla/Firefox permet le blocage des hyperliens invisibles en dehors du domaine en cours de visite et qu'Opera permet de supprimer la mention de la page référante par laquelle transitent le détail du clickstream de l'utilisateur vers les firmes de cybermarketing. Ces fonctionnalités sont absentes de MSIE version 6.0

[10] L'idée est de transporter l'information à l'aide de la lumière plutôt que d'utiliser des fils électriques. L'avantage majeur de cette solution consiste à pouvoir s'affranchir de l'échauffement de plus en plus considérable produit par les micro processeurs actuels.

[11] Calcul réalisé sur base d'une extrapolation des chiffres fournis par l'Union Internationale des Télécommunications pour l'année 1999 (vu sur http://www.itu.int/ITU-D/ict/statistics/at_glance/Eurostat_2001.pdf en mai 2004)

[12] En 1980, cela eut nécessité au bas mot des millions d'enregistreurs avec autant de bandes magnétiques. A cet époque, il fallait un enregistreur pour enregistrer une conversation.

[13] Voir, par exemple sur www.hitachi.com le 400GB Deskstar 7K400

[14] Actuellement des débits de 2,5 à 10 gigabits par seconde sont classiques sur ce type de support.

S'il s'agissait d'enregistrer toutes les paroles d'un être humain, de sa naissance à sa mort, on peut calculer[15] qu'un simple disque dur de haute capacité y suffirait aujourd'hui amplement.

Dans le commerce, on trouve actuellement des systèmes de type walkman capables d'enregistrer le contenu de l'équivalent de plusieurs centaines de CD-ROM classiques au format MP3. Les appareils photos digitaux permettent de stocker des centaines voire des milliers de photos alors que la capacité du film chimique classique plafonne à 36 vues. A raison d'un megabyte par photo de haute définition, un disque dur de haute capacité pourrait aujourd'hui stocker de l'ordre de quarante mille photographies de haute qualité.

Le Registre National de la Belgique qui contient la démographie de tous les Belges de la naissance à leur mort ainsi que leurs professions, mariages, métiers et adresses successives[16], sans compter des données relatives aux étrangers résidents en Belgique, tiendrait aujourd'hui sans problème sur une cassette DAT de la taille d'une grosse boîte d'allumettes ou sur quelques DVD. Il pourrait intégralement être transmis par fibre optique en quelques dizaines de secondes.

On pourrait objecter que le stockage n'est pas tout et qu'il est difficile de pouvoir traiter cette masse d'information pour y retrouver des données particulières. Il n'en est rien pour deux raisons. D'une part, la loi de Moore s'applique aussi et d'abord à la vitesse de traitement des processeurs. D'autre part, les algorithmes d'indexation automatique et de reconnaissance des formes (« pattern recognition ») ont fait des progrès importants durant ces dernières décennies. Le temps nécessaire à la recherche dichotomique, par exemple, (typiquement retrouver une personne dans une liste alphabétique) évolue en fonction du logarithme en base deux du nombre de personnes présentes dans la liste. En d'autres termes, toutes autres choses restant égales par ailleurs, s'il faut une seconde à un ordinateur pour trouver une personne dans une liste alphabétique de mille individus, trois secondes lui suffiront pour retrouver cette même personne dans une liste d'un milliard d'individus.

2.4. UNE MODIFICATION SUBSTANTIELLE DE LA NATURE ET DE LA CAPACITE DES TERMINAUX DE TELECOMMUNICATION

Une autre (r)évolution majeure concerne les terminaux de télécommunication. Elle va de pair avec le développement foudroyant de la micro informatique. Au début des années 80, les appareils terminaux de télécommunication étaient unifonctionnels[17]. Depuis le début des années 1990, et notamment avec l'intégration du multimédia dans les ordinateurs personnels, il existe une convergence très forte entre les terminaux de télécommunication et les ordinateurs personnels. A l'heure actuelle, tous les terminaux de télécommunications sont des micro ordinateurs. Le problème est que, contrairement aux terminaux classiques (téléphone et téléfax) et aux protocoles (notamment la norme ISDN) d'antan qui étaient régis par une réglementation de l'Etat par le biais d'une agréation, les ordinateurs d'aujourd'hui ne font l'objet de normes que techniques élaborées par des ingénieurs embauchés par l'industrie des Technologies de l'Information et la Communication (TIC ou ICT). Si certaines contraintes sont prises en ligne de compte par cette industrie, ce n'est pas tant pour protéger la vie privée des citoyens (les entreprises qui achètent ces technologies ont des raisons nombreuses pour

---

[15] En supposant qu'un être humain vit cent ans, qu'il dort huit heures sur 24 et parle durant un dixième de son temps en moyenne, la capacité nécessaire à l'enregistrement de son discours durant toute sa vie s'élèverait à 263 gigabytes

[16] Soit environ 2 milliards d'octets

[17] Linguistiquement l'usage de l'appareil et son nom forme un même terme : *je téléphone, tu télécopies*

connaître *leur* clientèle ou *leurs* prospects) mais pour éviter une généralisation de la méfiance des consommateurs, méfiance qui serait préjudiciable au commerce.

2.4.1. Les terminaux : un changement des paradigmes sociaux de la communication

La caractéristique principale des terminaux de télécommunication se situe dans leur capacité naturelle (c'est dans la *nature* même de l'informatique) d'effectuer des copies et de garder une trace, un souvenir des communications effectuées. La nature même de l'équipement terminal qui est passé de l'électromécanique à l'électronique programmable conduit à un **changement de paradigme social** totalement implicite mais certain. L'appareil de télécommunication possède toujours un déterminisme qui n'est plus entièrement dicté par l'utilisateur mais bien par le concepteur de l'appareil.

En d'autres termes, la pression sur une touche ne provoque plus de manière quasi mécanique un changement d'état de l'appareil, changement d'état par ailleurs généralement observable (par exemple : décrocher le combiné et avoir une tonalité, entendre une sonnerie et décrocher le combiné) mais constitue l'appel à un programme informatique qui possède l'autonomie de faire ce que l'utilisateur demande, si le programmeur l'a décidé et de la manière dont il l'a décidé. Qui plus est, ce comportement peut être ***en tout ou en partie inobservable à l'œil nu***. Le terminal montre la vérité, mais pas toute la vérité. L'essentiel est invisible aux yeux et l'essentiel n'est pas ce qui apparaît sur l'écran mais bien ce qui rentre, ce qui sort et ce qui est stocké dans le terminal de télécommunication. C'est bien pour cette raison que les cookies ont soulevé tant d'indignation. Par défaut les cookies ne sont pas visibles, rentrent et sortent en catimini du terminal de télécommunication. Ils y sont stockés généralement à l'insu des internautes[18]. Il convient de relever qu'un mécanisme semblable avait été imaginé pour être installé à bord des terminaux TELETEL (l'ancêtre du terminal Minitel en France) durant les années 80[19]. Il s'agissait de mettre une mémoire dans l'appareil terminal qui aurait pu être utilisée par le serveur. Suite à une levée de boucliers des associations de consommateurs ainsi qu'à une recommandation adressée par la CNIL à l'opérateur, ce type de procédé avait été abandonné. Historiquement, les cookies sont apparus dans la version 2 de Netscape Navigator, Netscape en a publié la première spécification[20] en 1996. La version 3 d'Internet Explorer implémente ces spécifications. Depuis, les cookies ont fait l'objet d'une standardisation par le W3C[21] et par l'Internet Engineering Task Force[22].

---

[18] Nous considérons comme optimiste de considérer que 5% des internautes « de la rue » savent ce qu'est un cookie, quels risques ces cookies induisent et comment s'en défendre.

[19] C'est l'intervention de la CNIL elle-même qui a l'époque avait mis fin au développement d'un tel système (voir à ce sujet Marie Georges, Technology for Privacy Protection, p. 4 , 23ème conférence mondiale des Commissaires à la protection des données, Paris, 2001, disponible sur http://www.paris-conference-2001.org/eng/contribution/georges_contrib.pdf).

[20] http://wp.netscape.com/newsref/std/cookie_spec.html

[21] « HTTP State Management Mechanism » sur http://www.w3.org/Protocols/rfc2109/rfc2109 .

[22] « HTTP State Management Mechanism » disponible sur http://www.ietf.org/rfc/rfc2965.txt . Une phrase mérite d'être relevée : « *Neither clients nor servers are required to support cookies. A server MAY refuse to provide content to a client that does not return the cookies it sends.* »

L'idée même du bon vieux téléphone[23] s'oppose à ce modèle. Il possède des caractéristiques, qui, bien qu'évidentes méritent d'être signalées, peut-être justement parce qu'elles semblent aller de soi. En règle générale, toutes autres choses restant égales par ailleurs,

1. c'est l'utilisateur qui doit poser un acte positif et concret (décrocher, former le numéro) pour entamer une télécommunication. Le téléphone ne peut pas téléphoner sans l'acte positif d'un être humain ;

2. le fait qu'une communication est en cours est parfaitement observable du fait que le cornet est décroché ;

3. l'utilisateur du réseau peut mettre fin à une télécommunication à tout moment par un acte simple, positif et concret (raccrocher le combiné) ;

4. l'utilisateur sait en principe à qui il téléphone (la déviation d'appel n'était pas possible) ;

5. une télécommunication s'opère entre deux individus et un tiers ne peut pas prendre connaissance du contenu échangé entre deux personnes, sans installer de dispositif d'écoute ;

6. chaque interlocuteur entend tout ce qui se dit au téléphone. (il n'y a pas de canal de service inaudible sur lequel peuvent transiter des informations de service, comme dans le système ISDN).

On peut véritablement parler ici d'un paradigme de transparence et de parfaite maîtrise de la télécommunication, une manière universellement admise de communiquer. Il convient de souligner que la numérisation du téléphone (ISDN) a commencé à changer fondamentalement ce paradigme.

Avec des téléphones électroniques et ISDN en particulier il devient possible de téléphoner en mains libres, sans décrocher le cornet. Cette fonctionnalité a été introduite au niveau des centraux eux-mêmes afin de permettre les écoutes téléphoniques, non seulement d'une communication mais de la pièce ou se trouve un téléphone, sans décrocher le combiné[24][25].

---

[23] appelé en jargon POTS (Plain Old Telephone System)

[24] Ceci a été établi par le rapport du SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT du Parlement européen en 1998 en ces termes : « *2.5 ISDN. It is technically possible to tap an ISDN telephone with the help of software that remotely activates the monitoring function via the D channel, obviously without physically lifting the receiver. It is therefore easy to eavesdrop on certain conversations in a given room.* » in DEVELOPMENT TECHNOLOGY AND OF ECONOMIC Vol Encryption and cryptosystems a survey of the technology Working document Luxembourg, November 1999. Vu sur http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-3_en.pdf en mai 2004

[25] Le procureur Eva Joly qui enquêtait sur une affaire de corruption en fera d'ailleurs les frais : « *Un quart d'heure plus tôt la présidente de la cour d'accusation a tenté de me joindre. Mon téléphone n'a pas sonné, mais elle a eu la surprise... d'entendre en direct l'audition du PDG d'Elf-Gabon. Mon téléphone est devenu micro clandestin, utilisable en composant simplement mon numéro interne. Je dresse un procès-verbal d'incident à destination de mes supérieurs. Aussitôt, la rumeur court les couloirs que je suis devenue paranoïaque ou mythomane... (...) Ainsi en est-il parfois de nos journées : passer notre temps à prouver que nous ne sommes pas folles, pendant que des violations aussi graves de la loi - telles qu'enregistrer le contenu d'un interrogatoire ou placer un magistrat sur écoute - ne mobilisent que nous-mêmes et ne troublent personne au sein de la hiérarchie judiciaire. (...)* » in Eva Joly « Est-ce dans ce monde que nous voulons vivre ? » Edition Les Arênes, Paris, 2001

Un autre paradigme social est **l'initiative de la communication**. Dans le système téléphonique des années 1980, c'est l'utilisateur et lui seul qui décide de téléphoner (voire de répondre à un appel). Il ne serait pas possible qu'il en soit autrement, notamment pour trois raisons :

1. le fonctionnement de ce téléphone se caractérise par un contacteur électromécanique au niveau du combiné. Il faut décrocher pour avoir une tonalité et il faut avoir une tonalité pour composer un numéro ;

2. le service téléphonique est payant par le consommateur. Il ne serait pas acceptable qu'un tiers téléphone sur son compte ;

3. la plupart du temps, les appareils sont raccrochés. Si tout le monde occupait la ligne en même temps, le central téléphonique du quartier serait rapidement saturé.

Dans le modèle actuel, les terminaux (GSM, GPS, RFID, Internet, etc.) sont toujours actifs. La facturation se fait selon la durée de l'abonnement et plus du tout ou de moins en moins selon la durée de la communication. Comme ce sont des réseaux à paquets, il n'y a plus de phase préalable d'établissement d'un circuit de communication entre deux personnes. Il est même possible de communiquer avec de multiples interlocuteurs simultanément.

Ici encore, le cookie focalise au niveau symbolique ce changement de paradigme. Dans l'imaginaire social, surfer sur Internet relève d'un modèle « client/serveur » où une partie demande de l'information et où l'autre partie lui délivre l'information. Dans ce contexte, avec les nouveaux terminaux, il s'agit ici d'une **véritable inversion du paradigme client/serveur** : le terminal de télécommunication devient en fait un serveur de cookies à destination des autres ordinateurs du réseau Internet qui accèdent ainsi, comme des clients, à l'information stockée sur le terminal.

2.4.2. La complexité et l'opacité du fonctionnement des terminaux

La **programmation des terminaux de télécommunication** devient de plus en plus complexe et cette complexité est rendue possible par la miniaturisation. Chaque terminal est devenu une immense usine à gaz dont le fonctionnement global échappe même à son propre propriétaire. Par ailleurs, une tendance actuelle des terminaux de télécommunication consiste à mettre à jour automatiquement leurs programmes en se connectant sur le site du constructeur, ce qui signifie que cette complexité n'est pas stable dans le temps. En outre, pour les systèmes à code fermé, il est quasiment impossible de connaître les fonctionnalités de tel ou tel système ou de savoir tout ce qui se passe à l'intérieur d'un ordinateur.

Cette complexité présente un prix qui est payé par l'utilisateur. La sécurisation de versions successives ne se déroule pas, selon les règles de l'art du développement de logiciels, d'après un plan de test rigoureux et préalable à la mise sur le marché, mais bien par les utilisateurs, après la mise sur le marché.

Si l'on considère le respect de la vie privée comme une partie du génie logiciel, son intégration dans le produit de télécommunication présente un triple coût pour l'industrie des TIC.

1. Tout d'abord, il faut mettre au point des méthodes de suivi de qualité relatives à ce critère, ce qui retarde la mise sur le marché des nouveaux logiciels. En l'état actuel, ceci supposerait une réingéniérie complète des protocoles de télécommunication qui ont été conçus de manière naïve, sans anticiper les dangers actuels et en laissant la protection des données comme une option possible laissée à l'appréciation de l'industrie.

2. Deuxièmement, en rendant les terminaux de télécommunications moins bavards, on prive certaines sociétés commerciales d'informations de profilage précieuses et de revenus publicitaires en proportion avec leur « visitorat ».

3. Troisièmement, toute mesure de sécurité (et le respect de la vie privée en est une) représente en général une perte de rapidité et de fonctionnalité pour un bénéfice rarement compréhensible par les utilisateurs et inacceptable par les serveurs ou prestataires.

En pratique, les **terminaux de télécommunication sont devenus télécommandables à distance et extrêmement bavards**. De nombreux comportements des terminaux seraient aujourd'hui totalement inacceptables, s'ils étaient connus de leurs utilisateurs. Pour illustrer notre propos et démontrer l'exactitude technique de celui-ci, nous avons choisi de présenter ci-après l'analyse de bout en bout, de manière complète, précise et profonde des flux d'informations entre un internaute lambda qui consulte un journal en ligne et clique sur deux articles particuliers et le réseau.

Pour faire cet examen, nous avons nous aussi opéré un bien modeste changement du rapport entre l'utilisateur et le serveur. Nous avons en effet utilisé un « sniffer » de réseau. Il s'agit d'un type de programme largement utilisé par les administrateurs de gros systèmes informatiques pour examiner le trafic réseau et y détecter des attaques ou des anomalies. Dans notre approche, nous avons adapté cet outil pour le faire fonctionner sur l'ordinateur d'un internaute afin de visualiser le trafic entrant et sortant du terminal.

Il ne s'agit pas ici de faire le procès d'un journal en ligne particulier mais d'illustrer de manière représentative la manière de faire de nombreux sites actuels et surtout de montrer comment la technologie permet **en catimini** ce genre de comportement. Nous montrerons dans ce qui suit que le simple surf sur Internet à l'aide d'un programme de navigation classique ne répond plus à aucune de ces caractéristiques fonctionnelles du téléphone d'antan

En nous basant sur l'utilisation du protocole HTTP par les journaux en ligne, nous entendons démontrer que ce contrôle n'existe plus. Pour cette démonstration nous détaillons les flux effectifs lors de la consultation d'un journal en ligne. Ce que nous détaillons est le lot ordinaire et « quotidien » des lecteurs d'un journal en ligne mais peut être transposé à la visite d'un site portail ou d'un moteur de recherche.

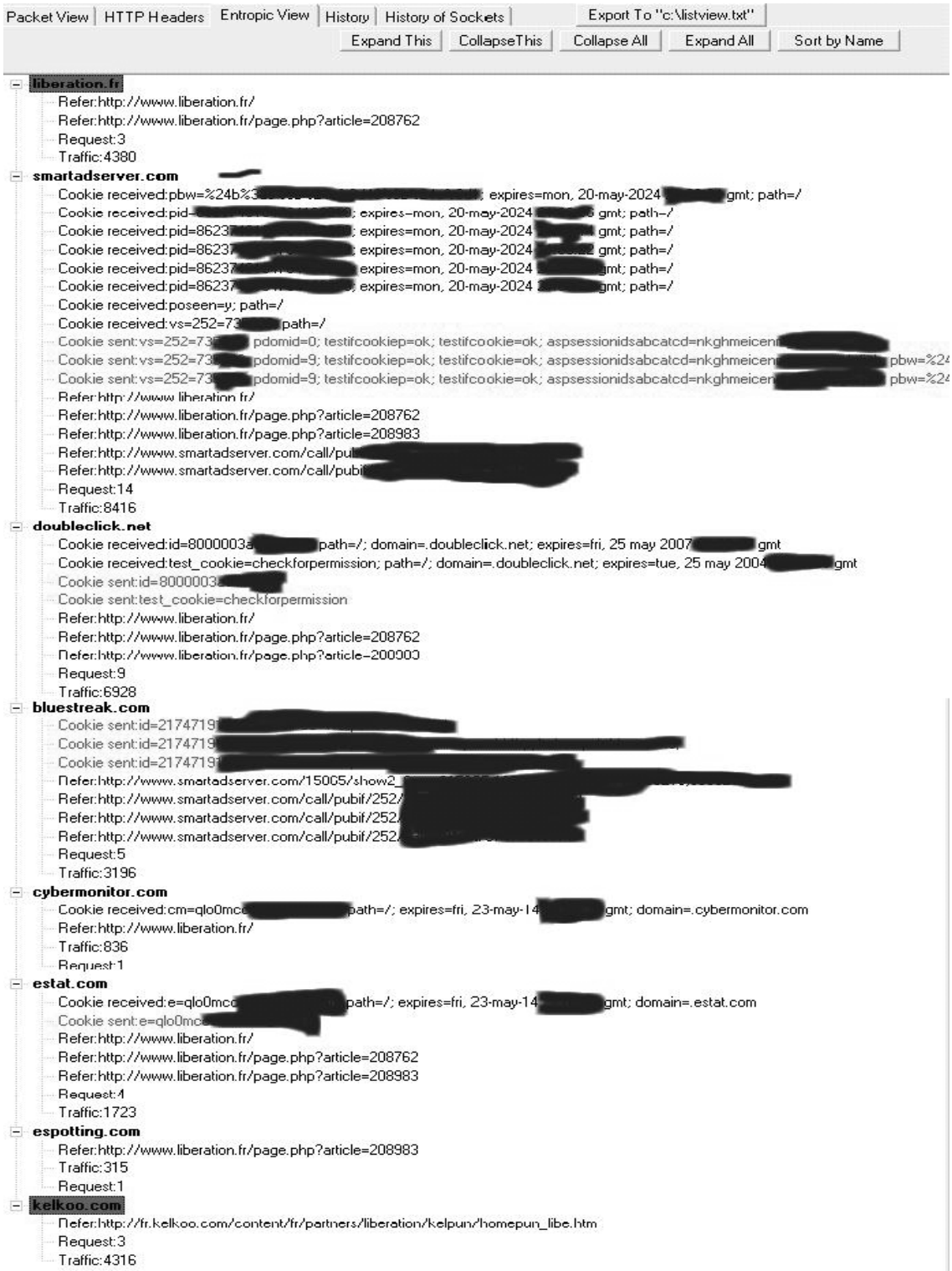
1. Le logiciel de navigation (Microsoft Internet Explorer 6) se connecte à la demande de l'utilisateur sur le site demandé mais aussi, à la demande du site visité par hyperliens dits invisibles, sur certains autres dont le journal en ligne a inséré la référence dans ses pages. L'utilisateur n'a aucun moyen d'empêcher ces connexions. Elles ne sont pas visibles et il n'en a pas conscience.

2. En se connectant sur ces sites tiers, le logiciel de navigation va, de manière invisible, dans son entête HTTP, indiquer la page référente, c'est à dire qu'il va communiquer à ce site tiers la référence exacte (URL) de l'article qu'il est en train de lire.

3. Lors de la réponse à ces requêtes HTTP invisibles de l'utilisateur, les sites tiers vont inscrire sur le disque dur de l'utilisateur, via la technique des cookies un numéro de série unique au monde que le logiciel de navigation va systématiquement rappeler lors de toute reconnexion à ce site tiers. Ce numéro de série unique au monde a une durée de vie de 3 à 30 ans.

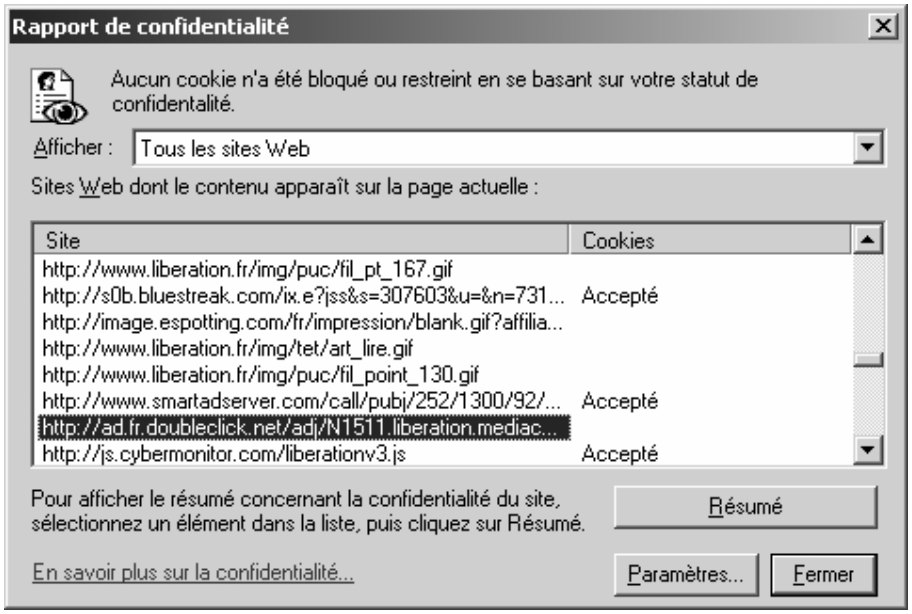
4. L'utilisateur a fait trois gestes positifs (taper l'adresse du journal et appuyer sur la touche entrée, cliquer sur un article puis sur un autre), le programme de navigation a effectué les

trois requêtes (pour un total de 4380 octets) mais le logiciel de navigation a aussi effectué 37 requêtes en catimini (pour un total de 25730 octets). Lors de ces 37 requêtes, il aura reçu dix nouveaux cookies identifiants, tout cela en moins de cinq secondes.



(Trafic effectif et invisible lors de la visite de la home page d'un journal en ligne et du click sur un article en ligne de ce journal. (Mai 2004)[26])

Notons toutefois que MSIE version 6 permet d'afficher un « rapport de confidentialité » sous la forme suivante[27]



Pour connaître la privacy policy d'un tiers, il faut donc afficher *après coup* cette fenêtre et cliquer sur le bouton résumé ; à ce moment apparaît la privacy policy dans une fenêtre étroite, non redimensionnable et non imprimable (un copier/coller n'est pas possible). A ce moment on peut observer la fenêtre suivante[28] :

Il est à noter que la simple lecture de cette privacy policy déclenche le téléchargement via HTTP d'une image sur le site du tiers en question (ici DoubleClick) qui peut donc ainsi connaître le nombre de fois que certains visiteurs ont lu cette privacy policy ainsi que certaines données les concernant.

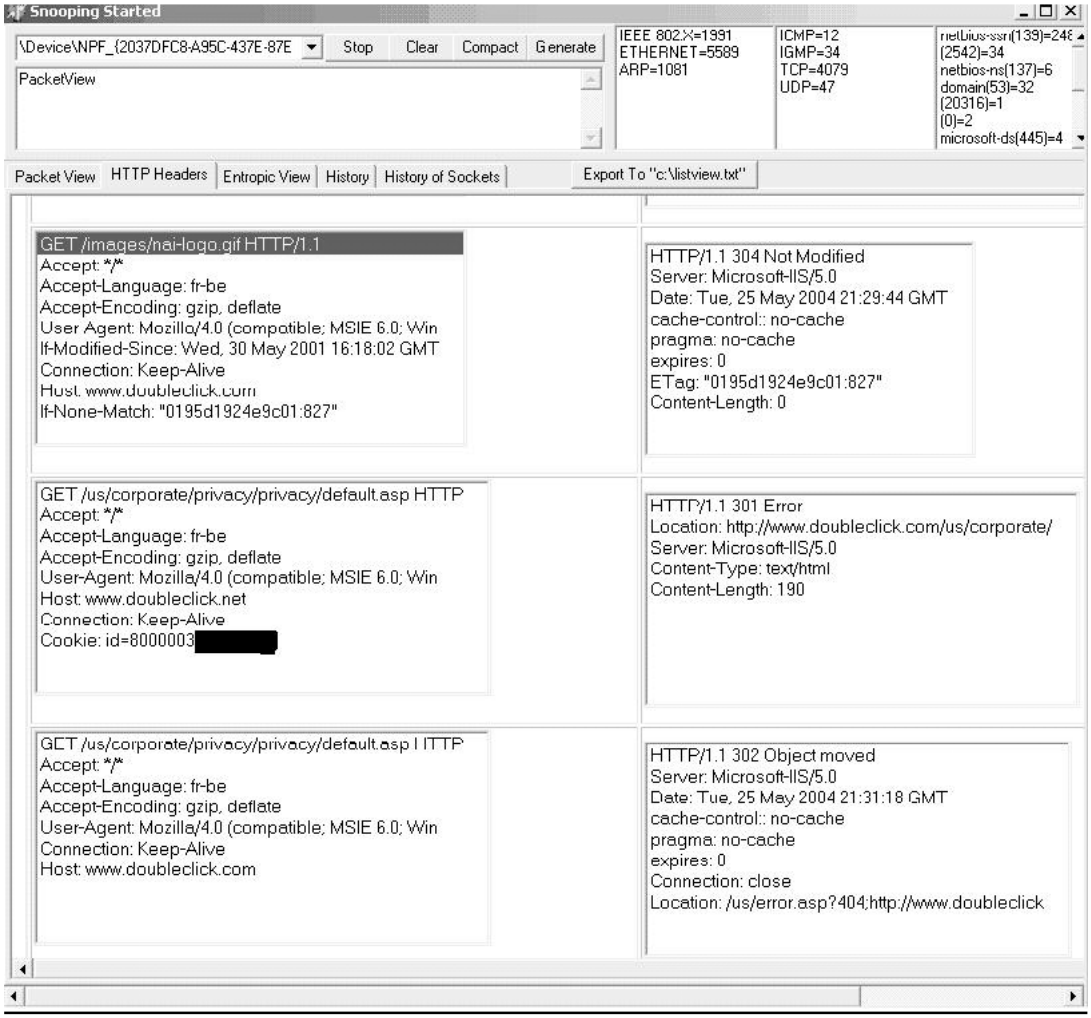
Si l'utilisateur désire avoir plus de renseignements sur la privacy policy, il peut cliquer sur un hyperlien qui avant de le diriger vers la privacy policy sur un site sans cookie, le fera passer par une URL particulière du tiers où son browser communiquera son cookie identifiant et unique au monde.

---

[26] Logiciel utilisé : Internet Explorer version 6 FR avec les dernières mises à jour (patches). Niveau de confidentialité et de sécurité réglé sur moyen (par défaut) avec vidage préalable du cache, effacement de l'historique et des cookies

[27] Il nous apparaît que l'internaute « de la rue » n'a ni le temps pour consulter *après coup* ce rapport, ni la compétence technique nécessaire pour l'interpréter.

[28] Pour des raisons techniques, la privacy policy complète se trouve en annexe.



Ceci démontre que l'intérêt de ces firmes ne se limite pas seulement à savoir sur une base individuelle les contenus accédés en ligne, les mots-clés tapés sur les moteurs de recherche ou les accès à des sites portails (via exactement la même technologie). Leur but ultime est aussi de connaître l'importance que les personnes attachent au respect de leur vie privée et leur niveau de compétence technique. A noter que les personnes souhaitant ne pas recevoir ce cookie identifiant de DoubleClick peuvent effectuer un opt-out. Techniquement, il s'agit d'autoriser DoubleClick à stocker sur le terminal un … cookie rémanent signifiant que l'on accepte pas d'autres cookies que celui-là. Ne serait-il donc possible de protéger sa vie privée qu'en se faisant ficher par une entreprise de cybermarketing ?

2.5. LE CAS PARTICULIER DES RFID

De manière insolite, les RFID (Identification par Radiofréquences), *comme les cartes à puces* naissent de l'application de la loi de Moore. Si la puissance des microprocesseurs augmente et si leur prix diminue, ceci entraîne, à puissance constante, une diminution phénoménale des prix des processeurs. Ainsi, certaines cartes à puces sont équipées du processeur qui équipait les célèbres Apple II au début des années 80. Ces ordinateurs que sont les RFID possèdent les caractéristiques suivantes :

- un processeur

- une mémoire morte
- une antenne qui permet tout à la fois de communiquer avec un terminal et de recevoir l'énergie requise pour faire fonctionner l'ordinateur (il n'y a donc pas de piles)
- absence de périphériques d'entrée/sortie accessibles à un être humain
- très haut degré de miniaturisation (de l'ordre de quelques millimètres, antenne incluse)

Le marché des RFID's se déploie à une échelle mondiale pour identifier et tracer la plupart des biens matériels. On a cité comme cas les chemises Benetton ou les rasoirs Gillette[29].[30]. Les arguments généralement avancés sont la lutte contre le vol en magasin et un environnement ambiant plus intelligent qui permettrait aux objets même les plus insignifiants de communiquer avec leur utilisateur. Une autre utilisation possible est constituée par le numéro de série qui pourrait être gravé dans cette puce scellée dans l'objet.

Par contrôle, nous entendons une triple capacité effective et pratique[31] :

1. de voir et de comprendre ce qui est transmis (envoyé et reçu) sur la ligne par un terminal ;
2. s'opposer à la transmission d'un contenu (envoi ou réception) sur la ligne par un terminal ;
3. si possible, réparer une transmission erronée.

A l'instar des cookies, les puces RFID posent problème aux défenseurs de la protection des données parce qu'elle se caractérisent par leur opacité qui a atteint ici un niveau maximum : Les puces RFID constituent l'exemple extrême de l'absence de contrôle de l'utilisateur sur son terminal de communication : il ne peut pas savoir si ce terminal est présent, où il se trouve, ce qu'il contient ou ce qu'il transmet. Il n'est même pas capable de l'allumer ou de l'éteindre. Aucun élément observable ne témoigne ,de ma mise en route de la puce RFID.

En conclusion, il est devenu et il deviendra de plus en plus possible et de moins en moins VISIBLE d'enregistrer la vie de tous les individus de la planète.

---

[29] L'ambition sous-jacente est à terme de pouvoir identifier de manière uniforme au niveau mondial la totalité des objets produits par l'industrie et la tentation corollaire de pouvoir identifier de manière permanente les êtres humains et d'effectuer une corrélation entre ces deux énormes banques de données est évidemment bien présente. Comme le résume le remarquable rapport de la CNIL sur ce sujet : *« A l'échelle du globe, l'enjeu est de coder 50 à 100 000 milliards d'objets, sachant qu'un être humain est entouré d'environ 2000 objets en moyenne. »*

[30] Le système de codification des RFID est révélateur de son ambition. Le code EAN (European Article Number) se compose de 96 bits dont les 36 derniers sont réservés pour le seul numéro de série de l'article. Il s'agit donc de permettre donc l'identification individuelle de 16 milliards d'objets identiques (du même type et produits par la même firme). Si on ne voit pas quelle entreprise pourrait produire 16 milliards de produits identiques ni l'utilité de différencier le cas échéant ces milliards d'objets identiques, on notera qu'il s'agit de l'ordre de grandeur de la taille prévisible de la population mondiale dans les décennies à venir.

[31] En sachant qu'en théorie, la pratique se déroule comme la théorie mais qu'en pratique, la pratique ne se déroule jamais comme la théorie

3. Les acteurs

Aux considérations sur ce développement technologique, on ajoutera deux réflexions complémentaires sur la position de deux acteurs : les personnes concernées, d'une part et l'Etat, d'une part, et les opérateurs de télécommunications, d'autre part..

3.1. L'ABSENCE DE POLITIQUE DE CONTROLE DES TIC PAR LES GOUVERNEMENTS

Le réseau téléphonique possède une longue tradition de protection de la vie privée. Lors du déploiement du téléphone digital (ISDN), une attention toute particulière avait été apportée à l'efficience de certains services (notamment le masquage du numéro de la ligne appelante[32]). La mise en œuvre de ces services complémentaires était inscrite dans la norme technique elle-même et l'adhésion à ces normes techniques était une condition nécessaire à l'agrément des terminaux de télécommunication, et donc, à leur diffusion.

Les télécommunications sur Internet ont été rendues possibles par le développement de la micro informatique et la digitalisation des réseaux mondiaux de télécommunication. A l'opposé de l'appareil téléphonique, malgré une convergence fonctionnelle entre ces deux types d'appareil et la similarité d'usages qu'ils permettent, l'ordinateur personnel, son hardware, son système d'exploitation et ses logiciels de télécommunication ne font l'objet d'aucune réglementation opérationnelle et fonctionnelle liée à certaines exigences en matière de confidentialité et de contrôle par l'utilisateur. Cela ne signifie pas qu'un contrôle quelconque par un utilisateur averti s'avère toujours impossible mais plutôt que ce contrôle est complexe et reste limité à certaines opérations.

La maîtrise partielle des terminaux et de leurs fonctionnement caché n'est accordée par l'industrie qu'au compte goutte et bien souvent sous la pression populaire relayée par les média. Les programmes de navigation demeurent, au regard d'un expert en protection des données, bien inégaux. Si tous incorporent aujourd'hui des systèmes pointus de gestion des cookies (en distinguant les cookies issus de sites tiers des autres), l'envoi de la page référante vers des sites tiers n'est toujours pas pris en compte par le programme de navigation le plus courant et ce dernier prévoit toujours, par défaut, de permettre à des sites tiers de stocker un identifiant mondial unique sur le terminal de télécommunication de l'internaute.

3.2. L'ABSENCE DE STATUT DES NOUVEAUX OPERATEURS DE TELECOMMUNICATION

Dans les années 80, le trafic téléphonique, tout comme le courrier postal, étaient majoritairement gérés par des opérateurs nationaux (à tout le moins en Europe) qui jouissaient majoritairement depuis des décennies d'une tradition et d'une situation de monopole.

Le développement d'Internet et la libéralisation du secteur des télécommunications ont provoqué l'apparition de nouvelles entreprises qui constituent autant d'acteurs nouveaux. Ces acteurs sont en charge de l'acheminement des télécommunications mais sont soumis à une réglementation formelle moindre que leurs prédécesseurs.

---

[32] CLIR pour Calling Line Identification Resctriction.

Actuellement, n'importe quelle entreprise peut devenir un fournisseur d'accès à Internet et être ainsi en position technique pour observer ou enregistrer des télécommunications. Le respect de normes contraignantes en matière de protection des données ne pourra devenir effectif que si l'on assiste, parallèlement, à la professionnalisation du secteur des intermédiaires de télécommunication, ce qui suppose une formation, un accès conditionnel au marché et un contrôle.

4. Conclusion de la partie I

Les deux dernières décennies ont vu se succéder à une vitesse effrénée un nombre impressionnant d'innovations et de tendances technologiques qui ont façonné un réseau mondial de télécommunication. Ce développement technologique s'est opéré de manière internationale, sans qu'aucun gouvernement ou mouvement citoyen n'y prenne une part décisive et sans que les problèmes de diminution de la vie privée engendrés par ces réseaux ne soient techniquement abordés ou résolus. Caractérisons ces développements :

- **Des réseaux convergents et polyvalents et omniprésents dans la vie quotidienne**

Le réseau est polyvalent et tend à fédérer tous les réseaux de télécommunication existants. Il a envahi notre environnement et pénétrera chaque jour encore d'avantage de nombreux domaines et les objets qui nous entourent. De nombreuses activités qui hier se déroulaient sans réseaux de télécommunication nécessiteront demain l'utilisation de ces réseaux. Il n'est plus du tout déraisonnable de penser que, dans quelques années, la plupart des frigos seront dotés d'agents intelligents qui auront une connaissance parfaite des aliments stockés dans leur sein et de leur date de péremption (grâce notamment aux puces RFID). Ces frigos devenus « intelligents » pourront même prendre l'initiative d'afficher sur la télévision familiale des publicités ciblées, voire prendre contact directement avec des supermarchés pour recueillir des offres ou carrément passer commander de produits. De manière générale, il existe une tendance très nette de rendre les objets qui nous entourent plus intelligents en les dotant d'un terminal de télécommunication.

- **Des terminaux intelligents au fonctionnement opaque et complexe permettant une protection des données optionnelle.**

Ces terminaux de télécommunication sont aujourd'hui, dans leur très grande majorité, des ordinateurs. De par leur nature informatique et par implémentation, ces terminaux génèrent de manière totalement invisible de nombreuses traces des télécommunications qui transitent par leur biais. Ces traces sont soit stockées dans le terminal, soit envoyées sur le réseau, généralement sans en informer l'utilisateur. Les moyens techniques mis à la disposition des utilisateurs sont partiels, trop complexes et configurés par défaut de manière préjudiciable à la protection de la vie privée des internautes. Le respect de la vie privée est devenue une option accessible à ceux qui ont le temps et qui savent. La relation de l'individu par rapport à la protection de ses données est elle-même devenue une donnée à caractère personnel que de nombreux acteurs souhaitent posséder.

Les terminaux de télécommunication intègrent divers identifiants techniques qui permettent de « tracer » le comportement d'un individu sur le réseau. Ce traçage n'est majoritairement pas considéré par l'industrie comme une violation de la vie privée des individus tant que celui-ci n'est pas identifiable par un point de contact. La technologie des cookies permet à un site tiers, par défaut, d'injecter en catimini son propre numéro identifiant

dans le terminal et ce de manière durable, de manière à pouvoir suivre le comportement d'un individu sur Internet.

Les protocoles de télécommunication n'intègrent pas la protection des données comme une exigence essentielle mais comme une option généralement laissée à la libre appréciation des constructeurs de matériel et de logiciel intégrant ces normes.

- **Des opérateurs nouveaux venus**

Les opérateurs de télécommunication sont des nouveaux venus sur le marché et manquent de professionnalisme et de formation par rapport à la privacy. Il n'existe aucune règle contraignante permettant de faire de la connaissance de la protection des données une exigence essentielle incontournable pour l'accès au métier d'opérateur de télécommunication.

Piste de réflexions à propos de la première partie

En définitive, ce n'est qu'en définissant un modèle opérationnel de protection des données et en imposant des exigences fonctionnelles pour les terminaux, les protocoles et les opérateurs de télécommunication que la protection de la vie privée sur le réseau des réseaux fera un pas décisif vers tous les utilisateurs pour cesser d'être un privilège partiellement octroyé sur demande à une minorité avertie, revendicatrice…et identifiée.

II. L'ENVIRONNEMENT TECHNOLOGIQUE NOUVEAU INVITE A REFLECHIR SUR LE SENS A DONNER A CERTAINS CONCEPTS ET DISPOSITIONS DE LA CONVENTION.

Il s'agit ici de répondre à la question clé : avons nous besoin d'une législation spécifique en matière de protection des données dans la société de l'information, distincte de celle de la Convention n°108 et de son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données, protocole adopté le 8 novembre 2001 ou suffit-il d'approfondir les principes de cette Convention pour couvrir adéquatement les questions nouvelles de protection des données liées au développement des technologies de l'information et de la communication ?

Notre réponse part du texte de la Convention et suit la structure y proposée. Nous avons également voulu tenir compte dans notre jugement critique de textes récents plus spécifiques à l'environnement technologique nouveau créé en particulier par le développement de l'Internet. La Recommandation N° R(99) 5 du Comité des Ministres aux Etats membres sur la protection de la vie privée sur Internet adopté le 23 février 1999 et la Directive 2002/58 de l'Union Européenne concernant le traitement des données à caractère personnel dans le secteur des communications électroniques ont naturellement été prises en compte dans la mesure où elles représentent une première prise en compte de cette réalité nouvelle. Comme nous le verrons, certains aspects développés par ces textes nouveaux induisent la consécration de principes nouveaux, ce qui sera l'objet de notre troisième partie.

1. Article 1 - Objet et but de la Convention

1.1.L'OBJECTIF : LA PROTECTION DES DONNEES : AU-DELA DE LA VIE PRIVEE ?

« Privacy has a protean capacity to be all things to all lawyers » [33]

1.1.1. D'un débat : Vie privée à un débat sur les libertés

La définition de l'objectif de la Convention n°108: « le respect à toute personne physique de ses droits et libertés fondamentales, et notamment de son droit à la vie privée » ne devrait-il pas mieux mettre en évidence l'étendue des préoccupations exprimées par le concept de droit à la protection des données ? A cet égard, la doctrine[34] note le passage d'une approche négative et restrictive, où la vie privée est considérée comme un concept défensif et réducteur (données sensibles) permettant la protection des citoyens contre l'action de l'Etat et contre les atteintes à la confidentialité des données traduite par l'article 8 de la Convention Européenne des Droits de l'Homme (C.E.D.H.), à une approche plus positive et singulièrement plus large, définie comme droit à l'« autodétermination informationnelle », par l'attribution de droits subjectifs nouveaux à l'individu (droit d'accès, …) et la définition de limites au droit de traiter des données dans le chef tant des acteurs publics et privés (finalité légitime, proportionnalité, sécurité, …).

---

[33] T. GERETY, "Redefining Privacy*",*12 *Harv. C.R-C.L.L. Rev*. 233-234 (1977).

[34] Entre autres, D.J. SOLOVE, "Conceptualizing Privacy*"*, 90 *California Law Review*, 2002, 1085 et s.; P.BLOK, *Het recht op privacy,* Boom Juridische uitgevers, 2003.

La Convention n°108 traduit incontestablement cette approche plus positive en renforçant les moyens de contrôle par les citoyens des traitements opérés à propos de leurs données par l'octroi des droits à l'information et d'accès et en définissant des limites au droit à l'information des maîtres du fichier. Cette approche suffit-elle ou faut-il suggérer, sans s'écarter des termes de la Convention, une troisième approche ?

Comme nous l'avons noté, les technologies, plus par implémentation que par nécessité, génèrent et conservent les « traces » de l'utilisation des services et autorisent, par des capacités de traitement sans commune mesure avec celles existantes il y a à peine dix ans, une connaissance de l'individu et de ses comportements, individuels ou collectifs, personnels ou anonymes. En d'autres termes, leurs utilisations accroissent le déséquilibre existant dans la relation entre ceux qui disposent de l'information et les citoyens, personnes concernées ou non. Sur base des renseignements collectées, des décisions collectives (par exemple, la fixation du taux de remboursement d'une maladie) ou individualisées (par exemple, le refus de l'octroi d'un crédit ou d'un service bancaire) seront prises.

La Charte européenne des droits de l'Homme (Traité de Nice, 2000) invite, en ce sens et au delà de ce sens, à mieux distinguer les concepts de vie privée (article 7) et de protection des données (article 8)[35]. Le premier concept, plus défensif, constitue l'approche négative déjà décrite : limitant le droit des maîtres de fichier à traiter des données sensibles et préservant l'intimité des personnes concernées : « *The right to be left alone* »; le second concept suppose la prise en compte, d'une part, des déséquilibres de pouvoirs entre la personne concernée et le maître du fichier engendrés par les capacités de traitement des données à disposition de ce dernier et, d'autre part, de l'impact que les traitements peuvent avoir sur les diverses libertés du citoyen : ainsi, celle de se déplacer, celle de s'assurer, celle de se loger, celle de trouver un emploi, celle de s'informer et de s'exprimer en toute transparence, etc…

Ainsi, la création, au sein de réseaux inter-entreprises ou inter-administrations, de bases de données permettant un profilage a priori des utilisateurs de services peuvent amener à les discriminer lors de la recherche d'un logement, de la recherche d'information, de la demande d'une couverture d'assurance ou de l'acquisition d'un ouvrage[36].

Piste de réflexion

Cette constatation n'exige t'elle pas une approche plus préventive et globale des phénomènes observés, approche centrée sur l'impact des technologies vis à vis des libertés humaines[37] ? Cette approche se fonderait sur le principe de précaution, principe

---

[35] Article 7 : « *Toute personne adroit au respect de sa vie privée et familiale, de son domicile et de ses communications »*

Article 8 :

« 1. Toute personne adroit à la protection des données à caractère personnel la concernant. ; »

« 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. »

« 3. Le respect de ces règles est soumis au contrôle d'une autorité de protection des données. »

[36] Sur ce dernier point, les pratiques de « discriminative pricing » d'Amazon, dénoncées par les associations de consommateurs américaines et abandonnées depuis.

[37] **Pour ne prendre qu'un exemple : le remplacement progressif des modes de paiement traditionnels par des paiements par des cartes de crédit dont les émetteurs sont en situation oligopolistique exigerait**

développé dans le domaine de l'environnement et qui vise également les risques collectifs. Il est clair que ce rôle de « Technology Assessment » est déjà joué par les Autorités de protection, en particulier le Comité consultatif. Nous plaidons simplement pour qu'une emphase plus grande soit mise sur le caractère préventif de l'intervention souhaitée et sur l'analyse des impacts des innovations mises ou susceptibles d'être mises sur le marché sur les diverses libertés collectives ou individuelles des citoyens.

1.1.2. De la préservation de la dignité humaine au delà de la protection des données à caractère personnelle ?

La Convention garantit la protection de la vie privée, des libertés et, au delà, la **protection de la dignité humaine.** La tradition constitutionnelle allemande ancre la question de la protection des données à caractère personnel dans le cadre du droit de la personne à la dignité humaine. L'invocation de la dignité humaine entend rappeler que l'Homme est un sujet[38] et ne peut être ramené à un simple objet de la surveillance et du contrôle d'autrui. Ce rappel de la dignité comme valeur fondatrice de la vie privée[39] est sans doute nécessaire au vu de certaines utilisations de la technologie.

Les systèmes d'information réalisent de manière croissante une surveillance globale des populations et des individus, créant un système de transparence des comportements des personnes qui peut s'avérer contraire à la dignité humaine[40].

Piste de réflexion

Nous nous devons de souligner que ces atteintes à la dignité humaine peuvent exister même sans qu'il y ait « traitement de données à caractère personnel » (ainsi, la caméra filmant la manière dont une personne X non identifiable essaie un tube de rouge à lèvres). Le fait que la dignité soit mise en cause par la collecte de données sur des individus même si aucun risque d'identification de ces derniers n'existe (au delà de leur comportement qui les identifie de manière biographique (voir infra), doit amener à s'interroger sur l'intérêt d'appliquer les principes de la convention à ce type d'atteintes. Les principes de légitimité et de proportionnalité des traitements, le droit à une information des personnes dont les données sont collectées ne sont-ils pas à rappeler également dans ce contexte ?

---

une réflexion sur l'impact que peuvent avoir sur les citoyens tantôt le retrait ou le blocage d'une carte de crédit en termes de liberté de mouvement, tantôt l' analyse des utilisations de la carte en termes de surveillance globale des activités de l'individu.

[38] Cf. la célèbre phrase de Kant, parlant de la dignité humaine: " Il (l' homme) ne peut être regardé comme un moyen pour les fins d'autrui, ou même pour ses propres fins mais comme une fin en soi, c'est à dire qu'il possède une dignité par laquelle il force au respect de sa personne, et qui lui permet de se mesurer avec chacune d'elles et des 'estimer sur le pied de l'égalité. » (Doctrine de la vertu, p.96-97) citée par J. FIERENS, « La dignité humaine comme concept juridique, *Journal des tribunaux,*2002, p. 78.

[39] Sur cette relation, lire J.H. REIMAN, "The Right to Privacy ", in *Philosophical Dimensions of Privacy* 272, F.D. Schoeman ed., New York, 1984, 300 et ss.

[40] On cite le cas du londonien filmé 300 fois par jour par des caméras de vidéosurveillance ou le cas de l'employé portant un badge permettant de le localiser à tout moment pendant les heures de travail et d'ainsi déduire ses relations de travail ou autres avec d'autres employés eux aussi « badgés ».

1.1.3. Vie privée comme support ou mise en cause d'autres libertés

Que la vie privée ou de manière plus large la protection des données soit une garantie de nos libertés, cela va de soi. Ainsi, pour parler de la liberté d'expression et d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveiller dans ces communications et ne puisse à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de mes messages. La liberté de s'informer suppose que l'information ne soit pas filtrée, que je ne sois pas conduit, profilage aidant, à mon insu ou malgré moi, vers l'information qu'autrui souhaite me voir consommer. Pire, la même technique de profilage peut amener ce dernier à me priver de certains services ou informations dont on estime qu'il est peu rentable de m' autoriser à y avoir accès. Ces exemples pourraient être multipliés vis à vis des différents libertés consacrées par la Convention européenne des droits de l'Homme. **La protection des données est indiscutablement le support de nombre d'autres libertés et les garantit.**

Il arrive cependant que le souci de protection des données heurte le développement d'autres libertés**.** En particulier, la protection des données doit être mise en **balance avec les impératifs de protection de la liberté d'expression et d'opinion.** Le préambule de la Convention le rappelle implicitement : « *Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières ; Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples.* », sans qu'aucune disposition de la Convention n°108 ne consacre cependant explicitement la nécessité de cette mise en balance[41]

Ce souci de ne pas attenter, par le biais de la protection des données, à la liberté d'expression et d'opinion a jusqu'à présent été approché par quelques dispositions protectrices du travail des journalistes y compris « électroniques ». Il apparaît de plus en plus que le problème est plus large dans la mesure où Internet offre à chacun (web logs, site personnel, etc.) d'affirmer son opinion et de faire part de ses activités y compris de ses relations avec des tiers.

Piste de réflexion

L'application des lois de protection des données avec les multiples obligations qu'elle crée vis-à-vis de ces tiers (obligation d'informer, etc.) crée un problème délicat vis-à-vis de cette liberté d'opinion et d'expression, qui pourrait ainsi se voir restreindre. L'affaire Linqvist récemment tranchée par la Cour de Justice des Communautés européennes[42] illustre le propos. Peut-on sur Internet évoquer ses relations personnelles, associatives ou professionnelles sans devoir se soumettre aux exigences de la loi sur la protection des données à caractère personnel. La Cour rappelle le devoir, compte tenu des circonstances, d'apprécier la proportionnalité de la restriction à l'exercice du droit à la liberté d'expression qu'entraîne l'application de règles visant à la protection des droits d'autrui. La formule est vague et renvoie à un jugement de proportionnalité. Ce jugement peut difficilement mettre sur le même pied l'expression journalistique qu'elle soit sous format

---

[41] A l'inverse de ce qu' à propos des traitements « effectués aux seules fins de journalisme ou d'expression littéraire et artistique », stipule expressément l'article 9 de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, JOCE, n° L 281 du 23 novembre 1995, p. 31 et ss.

[42] CJCE 6 novembre 2003, publiée notamment in RDTI, 2004, p. 67 et ss. avec la note d'observations de C. de TERWANGNE qui aborde amplement cette question.

traditionnel ou sur Internet, pour laquelle des règles ont progressivement été dégagées[43] et la libre expression de chacun dont l'existence renvoie nécessairement à celle d'autrui. Sans doute des travaux devraient être menés sur ce point.

1.2. CHAMP D'APPLICATION : UN ELARGISSEMENT RATIONE PERSONAE ?

1.2.1. L'élargissement aux personnes morales

On sait que certaines législations d'Etats membres (Norvège, Autriche, Luxembourg, Italie dans une moindre mesure) ont élargi le domaine d'application de leurs lois de protection des données ou de certaines dispositions de ces lois, aux personnes morales. Cette extension correspond à une latitude laissée par l'article 3b de la Convention qui envisagent la possibilité pour des Etats d'élargir la protection « *à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité morale.* ».

Dans le contexte des développements réglementaires nouveaux, la question de l'extension se repose. Ainsi, la Directive 2002/58/CE entend faire bénéficier les personnes morales de certaines dispositions protectrices et ce au nom de leurs intérêts dits légitimes[44]. Cet élargissement concerne en particulier les dispositions relatives aux communications non sollicitées, au secret des communications et aux limites mises aux traitements des données de trafic et de localisation mais pas aux envois non sollicités ni à la réception de cookies ou autres logiciels espions[45]).

Les raisons de cet élargissement paraissent être de divers ordres. On évoque l'intérêt de garantir aux personnes morales certains droits octroyés par les législations de protection des données aux personnes concernées (droit d'accès, droit à l'information, droit de correction) lorsque le déséquilibre des pouvoirs informationnels entre les personnes morales et les maîtres des fichiers est trop important (cas des P.M.E vis à vis des banques, des sociétés d'assurance, des administrations,…). La volonté de protéger les personnes physiques, membres de ces personnes morales et en particulier leur liberté de s'associer est, sans doute, une première raison. Elle est déjà évoquée à propos des premières dispositions législatives nationales qui parfois soulignent la difficulté de séparer l'existence de la personne morale de celle de ses membres ou de certains d'entre eux.

En ce qui concerne la solution proposée par la directive, on peut songer à d'autres justifications : le traitement des données de trafic et de localisation permet à ceux qui les opèrent de connaître de manière importante l'activité des personnes morales et aggrave de manière sensible le déséquilibre de pouvoirs entre la personne morale et les responsables de traitement de telles données. Bref, c'est le risque encouru par les personnes morales d'être soumises, comme les

---

[43] A noter que les réglementations nationales varient sur la manière dont doit être atteint cet équilibre (Cf. à ce propos, la note de C. de TERWANGNE)

[44] Sur cette protection des personnes morales et des associations, lire en particulier L. BYGRAVE, *Data Protection Law,* Kluwer Law International , Information Law Series, Den Haag, 2002, p. 173 et ss.

[45] Cf. à ce propos, le raisonnement tenu par J. DHONT et K. ROSIER, Directive Vie privée et communications électroniques : premiers commentaires, *Revue Ubiquité-Droit des technologies de l'information*, 2003, n°15, p. 7 et s.

personnes physiques, au pouvoir de ceux qui disposeront de ces informations qui justifient l'application étendue des dispositions relatives aux abonnés, personnes morales. Le fait que les communications non sollicitées constituent un coût important tant pour l'abonné personne physique que personne morale expliquerait la même extension.

Piste de réflexion

Le bien fondé de cette extension aux personnes morales du bénéfice des législations de protection des données ou de certaines de leurs dispositions devrait être réévalué dans le contexte des utilisations nouvelles des réseaux. **En conclusion, il serait intéressant que le Comité consultatif confronte la réalité aux risques avancés pour justifier l'extension débattue et avise le Conseil de l'Europe sur la pertinence de cette extension.**

1.2.2. L'extension aux profils

Le second point est plus délicat : faut-il au delà de la protection des individus, prévoir une réglementation protectrice des profils[46] ? Le profilage s'entend de deux étapes : d'une part, la détermination d'une série de caractéristiques à propos d'un individu ou d'une collectivité d'individus en lien avec un ou des comportements opérés ou attendus et, d'autre part, le traitement subséquent de ces individus ou collectivités sur base de la reconnaissance de ces caractéristiques. Chacune de ces deux étapes est importante.

La possibilité de collecter des données relatives à des comportements présents ou passés, données personnelles ou anonymes, en quantités et qualités de plus en plus importantes et de les traiter de manière de plus en plus fine génère des risques de plus en plus grands de créer des profils et de prendre des décisions a priori par rapport à ces profils[47]. Ainsi, la manière pour un internaute de naviguer sur le site d'une entreprise peut être caractérisée par quelques critères qui permettront après quelques visites de le ranger dans une catégorie[48] ou une autre, d'afficher lors d'un contact une page de préférence à une autre[49], voire de lui refuser tel service.

---

[46] A noter que cette réglementation existe en Suisse et partiellement en Norvège. Sur ces points, lire L. BYGRAVE, op.cit., p.185 et s.

[47] R.A. CLARKE, « Profiling : A hidden Challenge to the Regulation of Data Surveillance" , 4 *J. of Law and Information Science,* (1993), p. 403 et ss.

[48] Dans de nombreux cas, notamment en marketing, le but de la statistique est de pouvoir dériver de certaines données observables préalablement agrégées la probabilité de certaines caractéristiques non directement observables. Dans le cas de l'octroi de crédit, les banques ont pour habitude d'effectuer un scoring basé sur un ensemble de questions anodines qui va leur permettre de déterminer si *statistiquement* le candidat emprunteur rentre bien dans le profil type du client solvable. Prenons un exemple au hasard. Une personne occupant un poste à durée déterminée, avec un salaire moyen décroche un emploi à durée indéterminée avec un meilleur salaire auprès d'un employeur solide. Il déménage pour être plus près de son travail et n'a pas encore le téléphone. En vue de l'octroi d'un crédit, trois questions lui sont posées :

Est-il depuis longtemps chez le même employeur ? Réponse : non

Habite-t-il depuis longtemps au même endroit ? Réponse : non

Possède-t-il le téléphone ? Réponse : non

Une conclusion semble s'imposer. La banque se trouve en présence d'un individu instable dans son emploi, instable dans son habitat et qui ne possède même pas le téléphone. C'est le profil type des individus qui ne remboursent pas leurs prêts. En d'autres termes, la banque a intérêt à refuser ce genre de client parce qu'*en moyenne*, ce sont ceux qui posent le plus de problème. Le fait qu'un cas particulier vienne contredire cette théorie n'enlève rien à sa rentabilité globale si le raisonnement est vrai en moyenne et si l'étude de cas marginaux représente un certain coût. En d'autres termes, les conclusions hâtives et sommaires (p.e. il a une Rolls Royce et donc il est riche) ayant pour effet d'exclure de l'accès à certains biens ou services des

Ce problème du partage du pouvoir lié au partage de l'information est aussi observable dans le domaine du profilage en ligne. L'ambition des sociétés commerciales n'est plus aujourd'hui de réaliser une simple vente, mais bien plutôt, à l'occasion d'une première vente, de parvenir à collecter un maximum d'information de manière à préparer les ventes suivantes. Des informations relatives à la clientèle permettent en effet de calculer l'élasticité de la demande et ainsi de faire varier, **de manière individuelle**, le prix. Amazon a ainsi été soupçonné de pratiquer *l'adaptative pricing* en utilisant des cookies identifiant le profil d'un acheteur particulier pour réviser ses prix à la hausse selon le profil supposé du candidat acheteur. En termes économiques, un prix unique n'est pas de nature à maximiser le profit d'une entreprise puisque la plupart des acheteurs possèdent des courbes d'élasticité différentes. La maximisation du profit est atteinte lorsque chaque produit est vendu au prix maximum que chaque individu est prêt à payer. Dans le cas contraire, le consommateur jouit généralement de ce que les économistes appellent une rente qui est l'avantage qu'il reçoit en payant un bien à un prix déterminé alors qu'il était prêt à payer un prix supérieur. En termes de pouvoir économique, le profilage est une technique qui peut permettre au vendeur de s'approprier la rente du consommateur pour ainsi maximiser son profit

Cette lecture de la convention en termes d'équilibre des pouvoirs générés par l'information relative aux individus montre bien que l'objectif de rééquilibrage poursuivi par la Convention ne saurait être atteint si l'on extrait purement et simplement les profils « anonymes[50] » du champ d'application de la convention.

En matière publique, des centres d'expertise et des institutions statistiques sont chargés de même de collecter à partir de sources variées des informations de nature diverse pour établir des profils et aider ainsi les autorités publiques à prendre leurs décisions ou à contrôler le respect de leurs décisions[51]. Il sera ainsi possible d'établir le profil du fraudeur et d'alors identifier dans des bases de données multiples et, le cas échéant, croisées, les personnes à surveiller dans le cadre d'une législation de sécurité sociale ou fiscale.

Piste de réflexion

Il est donc important qu'indépendamment du caractère personnel des données traitées, certaines règles soient posées à propos de l'établissement de profils (première étape), indépendamment de leur application ultérieure dans une seconde étape à des personnes

---

personnes présentant des caractéristiques objectives trouvent leur justification du point de vue économique du profit maximum, même si elles créent ça et là des exclusions non fondées. Il suffit que l'exclusion, dans son ensemble, soit rentable. Il est clair que le profilage à outrance permet et permettra ce genre d'exclusion d'une manière automatique, sans recours sérieux de la part de l'individu atypique. Les statistiques sont dans de nombreux cas des données personnelles lorsqu'elles sont « réappliquées » à un individu, sur base de certaines de ses caractéristiques observables pour en déduire d'autres qui ne le sont pas.

[49] Ne serait-ce que la page d'accueil dans la langue de l'internaute de manière à lui éviter de devoir rappeler à chaque fois ce choix mais également de sélectionner les news ou les publicités en fonction de ses goûts, voire de lui proposer les prix des services ou bien en fonction des caractéristiques de son profil. A noter que les internautes sont parfois invités à aider le prestataire à mieux le cibler afin que celui puisse répondre plus adéquatement à ses besoins de tous ordres y compris sexuels. Ce profilage a priori de plus en plus fin est la base de tout le développement du one to one marketing.

[50] Sur cette notion, voir l'ambiguïté de la notion d'identité telle que détaillée infra nos réflexions à propos de l'article 2 a) de la Convention.

[51] Sur ces applications, lire l'article prophétique de J.BING, "Three Generations of computerized systems for Public Administrations and some implications for Legal Decision Making", 3 *Ratio Juris* 1990, pp. 219 et ss.

physiques[52]. **A cet égard, ces règles peuvent être dégagées des principes des législations modernes de protection des données : ainsi, on pourrait songer à une obligation de celui qui établit les profils d'informer la collectivité visée sur la logique du traitement avant même toute application. Les principes de légitimité et de compatibilité des finalités quant à l'utilisation des profils envisagés, celui de proportionnalité des données récoltées pour caractériser ces profils pourraient également s'avérer relevants, de même que les limites relatives à l'utilisation des données dites sensibles selon la Convention . Enfin, on pourrait songer à la transposition vis-à-vis d'acteurs privés de règles développées à propos de la statistique publique où des comités rassemblant des utilisateurs des statistiques, des représentants des autorités de contrôle etc. se réunissent pour analyser les programmes statistiques et leur bien fondé (principe de l'User Participation).**

2. Article 2 - Définitions :

2.1. LA NOTION DE DONNEES A CARACTERE PERSONNEL (ARTICLE 2.A)

La notion repose sur l'identification ou l'« identifiabilité » des individus concernés par ces données. En principe, la réglementation de protection des données n'est applicable que si la donnée traitée peut être référée à une personne déterminée[53]. Or la notion d'identité est peu évidente lorsqu'on la confronte à certaines réalités nouvelles. Ainsi, le RFID qui suit un vêtement[54] est-elle une donnée à caractère personnel alors qu'elle se rapporte directement du moins à un objet de même que le numéro IP qui se rapporte en définitive à un ordinateur et non à un utilisateur précis ? Sur ce point, nous confronterons trois regards avant de suggérer des pistes de réflexion.

2.1.1. L'identité : une notion ambiguë

La notion d'identité est ambiguë : elle peut signifier au moins trois choses différentes :

1. une caractéristique d'une personne qui est un trait de sa ***biographie***[55] (par exemple son âge, ses transactions, sa famille, ses hobbies, son employeur, sa qualification professionnelle, ses déplacements, ses achats, etc.)
2. un ***point d'ancrage***, c'est-à-dire un donnée **identifiante** (au sens informatique du terme) qui permettra de faire le lien entre plusieurs caractéristiques biographiques de la même personne (par exemple un cookie rémanent, un numéro de client, un numéro

---

[52] L'article 15 (1) de la directive européenne 95/46 relatif aux systèmes automatisés régule les profils certes mais au moment où ils sont appliqués à une personne particulière. L'article 15 (1) réclame que la personne vis à vis de laquelle une décision est prise sur base d'une décision automatisée soit au courant de la logique du système qui lui est appliqué et puisse contester l'application du raisonnement automatisé dans son cas particulier.

[53] En matière de « profils », nous avons montré que certains traitements de données peuvent être dangereux alors même que dans un premier stade, le lien avec des personnes déterminées n'est pas opéré dans la mesure où le résultat du traitement est par la suite (dans un second temps) appliqué automatiquement à des personnes déterminées et permet de prendre des décisions à leur propos.

[54] C'est l'exemple d'une des premières applications des RFID, les puces insérées dans les vêtements Benetton.

[55] Au sens étymologique : il s'agit de graver une tranche de vie. Bien évidemment *l'épaisseur* de cette tranche, ou, -plus scientifiquement-, la granularité des données aura toute son importance pour l'objet qui nous concerne.

identifiant le terminal[56], …) Le point d'ancrage n'est pas biographique en tant que tel mais un pointeur identifiant un endroit ou l'on peut stocker toutes les données biographiques comprenant le dit point d'ancrage. Ces pointeurs permettent de relier entre elles des données purement biographiques en regroupant en un seul profil des analyse comportementale d'une même personne en des lieux et à des moments différents.

3. un ***point de contact*** qui va permettre à un tiers de prendre l'initiative d'un contact avec un individu. (par courriel, par courrier, par fax, par téléphone,…).

Le temps qui passe influence la qualité de ces données. Ainsi, une adresse IP dynamique est un point d'ancrage durant un temps assez court. Le terme « adresse » est lui même ambigu car il signifie tout à la fois un identifiant d'une personne particulière à un moment particulier et un moyen d'entrer en contact avec lui.

Ces trois propriétés de l'information demeurent conceptuellement distinctes même si, en pratique, elles se peuvent se trouver fondues ou confondues dans la même information binaire. Dans le monde matériel, la vulnérabilité des adresses postales provient du fait que l'adresse postale (et même électronique, dans une moindre mesure) cumule les trois propriétés citées ci-dessus. Une adresse postale composé du nom, prénom, rue numéro et localité est tout à la fois :

- un élément biographique : en révélant à un tiers l'endroit où la personne vit et par effet de bord, son niveau de vie (par son quartier), son origine ethnique (nom)
- un point d'ancrage: en révélant la même adresse à plusieurs tiers, il est techniquement possible que ceux-ci mettent en commun leurs informations. Si plusieurs personnes habitent à la même adresse et ont le même patronyme, on peut imaginer qu'elle font partie de la même famille
- un point de contact: l'adresse postale permet n'importe qui d'envoyer du courrier à une personne précise.

2.1.2. L'identité interprétée de manière restrictive par l'industrie

A titre d'exemple non marginal de cette interprétation restrictive, on peut citer le cas d'Abacus/Double Click. C'est, semble t'il, la pression populaire qui aurait empêché la fusion entre les banques de données d'Abacus[57] et de Double Click. On ne peut d'ailleurs que s'étonner que la fusion entre les profils "anonymes[58]" de Double Click et la banque de données nominatives d'Abacus ait été techniquement possible. Cela signifie tout simplement que DoubleClick qui prétendait ne collecter aucune information relative à une personne identifiable possédait néanmoins un point d'ancrage permettant de faire le lien. Ce lien est bien probablement le fameux cookie identifiant que DoubleClick a installé sur des millions

---

[56] Typiquement l'adresse MAC, numéro de série unique au monde identifiant chaque carte réseau ou le numéro IMEI identifiant tout téléphone mobile et transmis sur le réseau, etc… historiquement on peut noter que Microsoft avait programmé Powerpoint, Word et Excel en 1998 pour stocker en catimini ce numéro unique au monde dans tout document créé par l'utilisateur.

[57] « a cooperative membership database, contains records from more than 1,100 merchandise catalogs, with more than 2 **billion** consumer transactions from virtually all U.S. consumer catalog buying households » lu sur http://www.abacus-direct.com en mai 2004

[58] http://www.doubleclick.net/company_info/about_doubleclick/privacy : " *DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address.*

d'ordinateurs personnels[59]. Il suffit qu'un hyper lien invisible soit présent sur un formulaire nominatif en ligne pour que DoubleClick puisse faire ce lien.

Une tendance actuelle de l'industrie consiste[60] donc à considérer des points d'ancrages et de simples données biographiques y associées comme étant des données se rapportant à un individu non identifiable[61]. Des points de contact stables dans le temps sont généralement admis comme étant des données à caractère personnel. En d'autres termes, la surveillance et la traçabilité d'un individu ou des biens qu'il utilise ou possède ne sont pas majoritairement perçues comme une atteinte à la vie privée si la personne n'est pas identifiable et reste anonyme (c'est dire si on ne connaît pas son nom ou si on ne sait pas la contacter)[62].

Comme si nos comportements n'étaient pas constitutifs en soi de notre identité.

2.1.3. L'identité interprétée différemment selon les lois nationales

Le Conseil de l'Europe et plus tard la directive européenne 95/46 déjà citée définissent la notion de ***données à caractère personnel.*** Il s'agit de "*données qui se rapportent à une personne physique identifiable ou identifiée*". Il reste donc à savoir ce que signifie "identifier". La directive 95/46 ajoute que *"est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale".* Relevons au passage la tautologie (une personne est identifiable si elle peut être …identifiée, notamment par référence à un numéro …d'identification). Le « considérant » 26 de cette même directive précise que, « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne".*

---

[59] DoubleClick délivre plus d'un milliard de bannières publicitaires par jour.

[60] La déclaration de confidentialité de Microsoft Update va dans le même sens. Après avoir déclaré que le site collecte les informations suivantes

1. Numéro de version du système d'exploitation
2. Numéro de version d'Internet Explorer
3. Numéro de version des autres logiciels pour lesquels Windows Update fournit des mises à jour
4. Numéro d'identification Plug and Play des périphériques
5. Paramètre régional et linguistique

La « privacy policy » de Microsoft disponible sur : http://v4.windowsupdate.microsoft.com/fr/default.asp (dernière visite, 15 mai 2004)spécifie que *« Le système d'exploitation Windows génère un identificateur global unique (GUID, Globally Unique IDentifier) qui est stocké sur votre ordinateur afin d'identifier celui-ci de façon unique. Le GUID ne contient aucune information permettant de vous identifier personnellement et ne peut pas être utilisé pour vous identifier.* »

[61] L'étude récente sur quatre ans de mise en application du Safe Harbor révèle la façon dont les entreprises américaines ont tendance à définir la notion de données à caractère personnelle comme la donnée permettant l'identification directe par le maître du fichier des personnes concernées (J. DHONT, V.PEREZ, Y. POULLET avec la collaboration de J.REIDENBERG et L. BYGRAVE, *Safe Harbour Agreement Implementation Study,* étude disponible sur le site*:* http://europa.eu.int/com/internal_market/privacy/index_en.htm. ….)

[62] Voir la Privacy Policy de DoubleClick : A la question : « Les utilisateurs ont-ils accès à leurs informations personnelles recueillies par le site Web ? », **le site répond : «** Aucune information d'identification personnelle n'est recueillie, aucune n'est donc accessible. »

Ces précisions n'empêchent pas une certaine confusion lorsqu'on considère l'interprétation qu'en ont faite différents pays européens de ces textes lors de leur transposition. A titre d'exemple, notons les transpositions opérées par la Belgique, le Royaume-Uni et la Suède.

La loi belge[63] définit comme données à caractère personnel *toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "personne concernée"; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*. Il s'agit d'un « copier/coller » du texte de la Directive.

La loi anglaise[64] est plus restrictive quant au champ d'application de la loi puisqu'elle pose que des "*données à caractère personnel signifient des données relatives à une personne en vie qui peut être identifiée (a) à partir de ces données elles-mêmes, ou (b) à partir de ces données et d'autres informations qui sont ou pourraient probablement être en possession du responsable du traitement*". Notons le lapsus. On pourrait dire que des données relatives à un individu ne sont pas des données à caractère personnel si le responsable du traitement ne peut pas identifier la personne concernée. Mais dans ce cas précis, il n'y a pas de données à caractère personnel. Sans données à caractère personnel, il n'y a pas de traitement et, partant, il ne saurait donc y avoir de « responsable de traitement »[65].

En Suède, le Swedish Personal Data Act 1998 définit une donnée à caractère personnel comme *« tout type d'information qui peut être « attribuable » de manière directe ou indirecte à une personne physique en vie »*[66]. De manière étonnante, nulle mention n'est faite ici de la notion d'identité. Implicitement, on pourrait croire que la loi suédoise (censée transposer la Directive européenne 95/46) considère qu'une information ne pourrait être attribuée à une personne physique en vie sans l'identification de cette dernière. Sur Internet, on pourrait imaginer un client tout à fait non identifiable (par exemple utilisant une chaîne de relais IP sans journaux de bord) qui se verrait attribuer quelques cookies non identifiants attestant son homosexualité et son intérêt pour des traitements contre le sida. Dans le cadre strict de la directive 95/46, la loi ne s'appliquerait pas à ces deux cookies parce qu'ils ne se rapportent pas à une personne identifiable. Toutefois, le site (par exemple un site proposant des devis d'assurance vie en ligne) qui reçoit ce visiteur et ses cookies pourraient conclure, à tort ou à

---

63 Loi du 8 décembre 1992, telle que modifiée par loi du 11 décembre 1998. Une version consolidée de cette loi se trouve sur le site de la Commission de protection de la vie privée (HTTP://www.privacy.fgov.be)

64 The UK Data Protection Act 1998 art 5 states that personal data means data which relate to a living individual who can be identified- (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller..."

65 Ici on ignore la précision introduite par le considérant 26 de la Directive 95/46. Cette ignorance provoque des dommages collatéraux: Imaginons le gérant d'un supermarché qui noterait uniquement le numéro de plaque des véhicules garés dans son parking, le type de véhicule et les dates et heures de départ et d'arrivée. En règle générale, il est peu probable que le gérant du supermarché puisse, à partir du seul numéro de plaque en sa possession, remonter jusqu'au nom de la personne. Ce genre de relevé ne serait donc pas concerné par la loi anglaise. Il n'y a pas de données à caractère personnel, donc pas de traitement et encore moins de "responsable de traitement". Il peut être généralisé; affiné et consolidé à l'échelle nationale et on dispose ainsi d'un système permettant de suivre à la trace les véhicules à travers les emplacements de parking sur tout le territoire national. On imagine alors facilement un tel système en ligne sur Internet dans un paradis des données et tout quiconque pourrait reconstituer l'itinéraire, voire l'emploi du temps de son voisin, de son patron, de son conjoint ou de son amant.

66 "All kinds of information that directly or indirectly may be referable to a natural person who is alive".

raison, qu'il a affaire à un homosexuel probablement sidéen. La loi suédoise pourrait par contre trouver à s'appliquer dans la mesure où la propriété "homosexuel probablement sidéen" est *attribuable*, au moment de la connexion, à une personne physique en vie, même si elle demeure non identifiable.

Pistes de réflexion

En conclusion, il est évident que le comité consultatif doit se pencher sur la notion de données à caractère personnel, notion qui est au cœur de la législation de protection des données et préparer à cet égard une recommandation sur le sens à donner à cette notion et ce en tenant compte des pratiques d'identification des prestataires de service sur l'Internet. A ce stade, quelques premières remarques :

1. Une définition des données à caractère personnel basée sur celle, -indéfinie et indéfinissable de l'identité, et celle, corrélative, d'anonymat, sont des notions ambiguës et non directement opérationnelles. Fonctionnellement, il faudrait parler de données biographiques, d'identifiants liés à des personnes ou à des terminaux (voire à des objets) et de points de contact.

2. Dans le cadre de la réflexion, on notera que considérer une donnée comme le cookie l'IP ou un GUI comme « donnée à caractère personnel » entraîne l'application des dispositions de la convention et dès lors l'obligation de traiter cette donnée ne serait-ce que pour permettre les droits d'accès, etc. alors même que cette donnée n'aurait pas normalement été traitée ? Par ailleurs, appliquer des dispositions comme l'obligation d'informer la personne concernée pourrait s'avérer impossible sans l'identifier.

3. Par contre, ne pas traiter l'IP et le G.U.I. comme donnée à caractère personnel poserait problème au vu des risques que l'utilisation postérieure de ces données représente en termes de profilage de l'individu voire de possibilité de la contacter. A cet égard, on relève qu'avec la combinaison d'outils de surveillance du trafic sur le web, on peut facilement cerner le comportement d'une machine et derrière celle ci de son utilisateur. On reconstitue ainsi la personnalité de l'individu pour lui appliquer certaines décisions. Sans même s'enquérir de l'« identité » de l'individu, c'est à dire son nom et son adresse, on peut caractériser ce dernier en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui appliquer certaines décisions dans la mesure où le point de contact de l'individu (l'ordinateur de l'individu) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes, la possibilité d'agir vis à vis d'un individu ne nécessite plus nécessairement la possibilité de connaître son identité. L'interprétation de la notion de données à caractère personnel doit refléter ce constat.

2.1.4. Le cas particulier des données de trafic et de localisation : un régime spécifique ?

Faut-il approcher les données de trafic et de localisation comme des données à caractère personnel appelant une réglementation spécifique ?

Ces données sont définies, par la directive européenne 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[67], comme suit :

- « données de trafic : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » ;
- « données de localisation : toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public. ».

A propos des données de localisation et de trafic, leur statut particulier dans la directive s'explique, premièrement, par la finalité a priori limitée dans le chef des fournisseurs de service de communication ou d'un réseau public de télécommunications : l'acheminement des messages à destination ou en provenance des usagers des services de communications électroniques, et, secondement, par le caractère dangereux du traitement systématique de telles données qui révèlent les déplacements, l'entourage habituel, les habitudes de consommation et de vie de ceux-ci . Enfin, on souligne que l'utilisateur de tel service, sauf dans le cas de services à valeur ajoutée, se trouve dans une position de relative faiblesse dans la mesure où l'utilisation du réseau suppose implicitement la génération, le stockage et la transmission de nombreuses données techniques dont le sens et l'utilisation potentiels lui échappent et dont il ne peut suivre facilement la trace (supra, notre réflexion sur l'opacité du fonctionnement des réseaux, Partie I, 2.4.2.).

Ainsi la Directive limite a priori les traitements de telles données à une seule exception près : le consentement dûment informé et révocable à tout moment de la personne concernée. Par ailleurs, le fait de subordonner au consentement de la personne concernée l'utilisation de ces données pour l'offre de services à valeur ajoutée ne s'explique t'il pas, notamment, par le fait que, dans la mesure où le consentement peut facilement être donné et retiré via l'utilisation même des technologies, il peut être considéré que ce consentement devient la base unique de légitimité des traitements relatifs à ces services supplémentaires.

Piste de réflexion

Sans doute, serait-il intéressant que la question particulière des données de trafic et de localisation soit rencontrée par une recommandation particulière pour les constructeurs d'appareils terminaux qui génèrent ces informations et pour les fournisseurs de réseau et de service de communication offerts au public qui les conservent.

Il s'agit de services qui consistent essentiellement ou principalement en la transmission ou la diffusion de signaux sur les réseaux électroniques.

L'ajout de cette définition permettrait d'introduire une réglementation de ces « fournisseurs » dont l'intervention est nécessaire entre l'émetteur du message et le destinataire (parallèle avec l'ancienne réglementation des transporteurs de courriers comme la Poste et les opérateurs de téléphonie vocale). Cette réglementation doit définir les moyens d'assurer le secret de la correspondance, les limites du droit au traitement des données de trafic et de localisation, obliger à la séparation des traitements opérés dans le cadre des services de communication de simple transport et les services à valeur ajoutée (parallèle avec les règles

---

[67] La recommandation n° R(99) 5 du Comité des Ministres du Conseil de l' Europe sur la protection de la vie privée sur Internet ne prévoit ni définition, ni réglementation particulière de ce type de données.

de l'O.N.P. en matière de réglementation des télécommunication), fixer les règles de la coopération entre autorités publiques et ces fournisseurs en cas de procédures de recherches d'infractions et enfin mettre à leur charge une obligation d'alerter les clients de leurs services des risques en matière de vie privée, liés à l'utilisation de ceux-ci.

2.2. LES NOTIONS DE FICHIER (ARTICLE 2 B)) ET DE TRAITEMENT AUTOMATISE(ARTICLE 2C))

La définition de la notion de traitement ne s'étend pas, selon le texte de la Convention, à l'opération de collecte des données. Est-ce une lacune ? On note en effet que l'article 5 prévoit que l'obtention des données doit être fait de manière loyale et que le traitement peut se comprendre du seul enregistrement de données. Or lorsque l'on collecte des informations sur la toile ou via un des protocoles de l'Internet, il y a toujours enregistrement au moins sur la mémoire RAM de l'ordinateur.

Piste de réflexion

Au delà de cette première observation, deux questions devraient être abordées.

Premièrement, la simple consultation de sites sur Internet (pure surfing) est-elle un traitement de données ou n'est-elle pas la mise en oeuvre de la finalité de celui qui a placé les pages sur Internet, à savoir plus particulièrement de l'opération de diffusion qui constitue la dernière phase du traitement ? On conçoit aisément que l'application de la loi de protection des données à la personne qui simplement surfe sur Internet soit irréalisable (obligation d'informer les personnes concernées, obligation de déclaration,…) et qu'en outre comme nous le montrons en répondant à la seconde question, il n'y ait pas nonobstant l'enregistrement éphémère des données, traitement de celles-ci.

Seconde question : nombre de pages de sites accessibles sur Internet contiennent des informations personnelles (images, textes, bandes sonores). La simple présence de cet ensemble d'informations rend-t-elle la Convention applicable ou faut-il que cet ensemble soit, dans une certaine mesure, organisé et structuré en fonction des personnes concernées ou du moins que des opérations logiques ou arithmétiques puissent être appliquées à l'ensemble de ces informations personnelles de telle sorte que les données relatives à une personne identifiée ou identifiable puissent être plus aisément rassemblées ? A notre avis, la simple visualisation séquentielle d'images (un match de football retransmis via Internet) n'est pas un traitement si des opérations relatives aux données personnelles y contenues (par exemple, un scanning permettant la reconnaissance automatique de personnes) ne sont pas possibles. Pour qu'il y ait traitement, il ne suffit pas qu'il y ait présence d'informations relatives à des personnes, il faut que des opérations puissent être appliquées à ces informations en tant qu'informations relatives à des personnes (principe de la valeur ajoutée). Sans doute, on objectera que nos ordinateurs disposent de plus en plus de logiciels applicatifs permettant de structurer a posteriori des informations au départ non structurées ou que de tels services sont offerts en même temps que l'accès à une base de données. Ainsi, les logiciels de recherche libre par mot ou nom autorisent l'interrogation de vastes ensembles de textes libres pour identifier les passages appropriés relatifs à une personne concernée. Leur présence voire leur application potentielle aboutissent alors à reconnaître l'existence de traitements. Confrontés à l'évolution constante de la technologie qui rend possible l'imaginable d'hier et rendra imaginable demain ce qui était inconcevable hier, nous ne pouvons que nous méfier chaque jour d'avantage du postulat fragile de l'impossibilité technologique de tel ou tel traitement.

2.3. LE « MAITRE DU FICHIER » (ARTICLE 2..D)

La définition de la notion de maître du fichier renvoie à l'analyse in casu du responsable de la définition de la (des) finalités du traitement, des catégories de données traitées et des opérations à appliquer. Dans le cadre des réseaux coopératifs, il n'est pas rare que les participants à ces réseaux confient des tâches d'intérêt commun à une entité chargée d'offrir des services à valeur ajoutée à l'ensemble des participants. Ainsi, des médecins d'hôpitaux et généralistes peuvent stocker leurs dossiers médicaux en un point central, faire transiter leurs courriers via cette entité qui offrira en outre des services d'archivage et d'horodatage, disposer auprès de cette dernière de ressources de traitement d'imagerie médicale, etc.[68]. Le statut de ces entités est difficile à appréhender au regard du concept de « maître du fichier ». Doit-on considérer qu'au regard de la variété des services qu'ils rendent, ils constituent des maîtres du fichier ou faut-il les considérer comme de simples sous-traitants, notion non aperçue par la Convention mais présente dans la Directive 95/46[69] ?

Piste de réflexion :

Cette définition et quelques principes quant à la responsabilité des sous-traitants et quant aux liens entre les sous traitant et le maître du fichier sont nécessaires au moment où se multiplient dans le réseau et parmi les services offerts par le réseau une multiplication des intermédiaires spécialisés et des situations qualifiables de sous-traitance.

Au delà, il serait utile de s'interroger sur la qualification de la personne, objet des données à caractère personnel comme maître du fichier ou en tout cas comme co-responsable du traitement dans certaines hypothèses où c'est la personne elle-même dont les données sont traitées qui définit la finalité et les moyens du traitement. Ainsi, la personne qui confie à un infomédiaire certaines données pour les voir traiter de manière à empêcher telle sollicitation commerciale, pour filtrer certains messages n'est-elle pas au sens de la Convention un maître du fichier recourant à un sous traitant en la personne de l'infomédiaire ? De même comment qualifier celui qui demande l'établissement d'un dossier médical pour pouvoir plus facilement disposer de ses informations vis à vis de médecins de son choix ? Les conséquences et l'intérêt d'une telle qualification doivent être étudiées soigneusement.

2.4. UNE NOTION NOUVELLE A AJOUTER : LA NOTION DE « PRODUCTEUR D'EQUIPEMENTS TERMINAUX »

Piste de réflexion

L'idée est d'ajouter à la présente Convention n° 108 un régime particulier imposant aux producteurs d'équipements terminaux (y compris les éléments logiciels intégrés dans le terminal) certaines obligations visant à la transparence de leur fonctionnement et empêchant des utilisations déloyales ou illicites de données à caractère personnel liées

---

[68] Sur cette réalité et l'intérêt de la notion de sous-traitance en la matière, lire J. HERVEG et J.M. van GYSEGHEM, « La sous traitance des données du patient dans la directive 95/46 », in Lex electronica, 2004, n°9 disponible à : http://www.lex.electronica.org.

[69] Cf. article 1 e) : *« sous traitant : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les, personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données. »*

aux opérations de connexion et de communication avec le réseau. A noter qu'ils ne sont pas en tant que tels visés par la présente directive, n'étant pas maître d'un fichier mais dans la mesure où le design de l'équipement qu'ils fournissent et les choix d'implémentation qu'ils effectuent autorise nombre de traitements, ils doivent être soumis à certains devoirs de manière à prévenir certains traitements que des tiers pourraient opérer de manière déloyale ou illicite et de transparence dans la mesure où l'utilisateur de l'équipement doit avoir une certaine maîtrise des flux générés par l'utilisation de son équipement (Cf. supra, Partie III : le droit pour l'utilisateur à la transparence du fonctionnement de son terminal)

3. Article 4 – Engagements des Parties

Le point 1 fait allusion aux « mesures nécessaires pour donner effet aux principes de base ». Il est remarquable qu'en 1981, le rapport explicatif d'une part, insiste sur l'importance de mesures destinées à rendre effectifs les principes qui risquent sans ces mesures de rester lettre morte et, d'autre part, appelle de ses vœux des mesures d'autorégulation comme garantie d'effectivité.

Ce souci de trouver des relais soit dans le développement de normes techniques[70] et de technologies de type Privacy Enhancing , les PETS[71], soit dans l'émergence de nouveaux métiers ou méthodes garantissant le respect des principes de la protection des données (label, infomédiaires, etc.) s'explique[72] pour divers motifs, particulièrement pertinents dans le monde de l'Internet :

- en raison de la plus grande **effectivité** de telles mesures qui, soit utilisent les ressources de la technologie pour imposer des solutions conformes aux requis de la protection des données (solutions technologiques)[73], soit reposent sur le consensus des acteurs intéressés pour trouver des solutions protégeant les données utilisations contraintes, abusives ou déloyales de ces technologies ;
- en raison du caractère **transnational** des solutions qui peuvent être développées dans ce contexte ;
- en raison de la difficulté pour les autorités de protection des données d'assurer seules ce respect ;
- en raison de la nécessité de créer un climat de confiance des usagers vis-à-vis d'un réseau considéré, à juste titre, comme « opaque ».

La conjonction des trois modes de régulation et leur bonne articulation constituent sans doute la bonne manière d'accroître la protection des personnes concernées et de les

---

[70] Voir à cet égard, les normes actuellement en discussion à l'ISO, « Security and Privacy »

[71] Privacy Enhancing Technologies :

[72] A cet égard nous renvoyons le lecteur aux considérations développées dans notre rapport de Prague, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », Conférence organisée par le Conseil de l' Europe, les 14 et 15 octobre 2004, à paraître. Cf. également, l'ouvrage de C.J. BENNETT et C.D. RAAB*, The Governance of Privacy,* Ashgate, 2003.

[73] J. REIDENBERG, « Privacy Protection and the interdependance of Law, Technology and Self-regulation »,in *Variations sur le droit de la société de l'information, Cahier du Crid, n° 20,* Bruylant, Bruxelles, 2002, p. 126 et ss.

sensibiliser[74]. L'exemple de « Privacy Policies » en témoigne. L'obligation légale de publier une page web relative à la pratique suivie en matière de protection des données, effectivement suivie par l'entreprise, accessible à l'utilisateur et conforme aux prescrits de la législation renvoie si on y regarde de près à quantité d'outils cette fois non nécessairement réglementaires. La réalité et la conformité de la pratique aux prescrits légaux peuvent être laissées à l'appréciation de certificateurs ou d'auditeurs[75] dont l'intervention sera annoncée par l'apposition d'un label. Les secteurs peuvent proposer des modèles de « Privacy Policies ». Pour éviter la disparité des formats, des modes d'expression et du vocabulaire utilisés, peut-être conviendrait-il de fixer une base minimum et un vocabulaire que ces différents labels devraient respecter, une sorte de meta label en quelque sorte. Le cas échéant, ne faut-il pas prévoir une intervention législative[76] qui pourrait fixer ces divers points.

L'accessibilité de la Privacy Policy sera réalisée par des applications logicielles qui feront en sorte que la page constituera un passage obligé et, le cas échéant, autoriseront à un système expert de comparer les « Privacy Preferences » de la personne concernée aux choix opérés par le responsable du traitement et relatés par la privacy policy. A noter que cette prise de connaissance d'une privacy policy doit s'opérer, a priori, de la manière la plus anonyme qu'il puisse être.

Un autre exemple est certes la régulation des labels de certification des sites web en matière de privacy[77]. La multiplication des labels induit la confusion de l'internaute. Quelle valeur accorder un label susceptible d'être copié, émis en terre lointaine par un émetteur inconnu dont l'indépendance n'est pas évidente, dont la qualité du contrôle des sites est douteuse et peu armé lorsqu'il s'agit de sanctionner un non respect aux règles du label. La labellisation des labels, c'est à dire le contrôle par une autorité publique ou par un organisme dont la composition atteste l'indépendance et la représentativité des divers intérêts peut être une solution que les autorités publiques peuvent mettre en place ou initier[78]

Piste de réflexion

Bref, les solutions sont à trouver, on le pressent, dans un subtil mélange, un système de co-régulation[79] où la loi trouve non seulement son prolongement mais également son effectivité dans des systèmes techniques et d'auto-réglementation qu'elle doit appeler de ses vœux et promouvoir. Ces diverses mesures de co-régulation ou d'auto-régulation ne

---

74 Sur ce point, lire J.R. REIDENBERG, « Lex informatica : The Formulation of Information Policy Rules through Technology », 76 *Texas Law Review* (1998)p. 553 et ss.

75 On peut concevoir que ces certificateurs et auditeurs soient eux-mêmes l'objet d'une accréditation selon un cahier des charges défini par une autorité publique ou en tout cas avec son aval. Cf. le parallèle avec le système TRUSTMARK UK. Sur ce système, R. DE BRUIN, XXX

76 Ainsi, 8 institutions fédérales américaines ont lancé la procédure d'Advanced Notice of Proposed Rulemaking (ANPR) réclamant des commentaires publics à propos de l'amélioration des « Privacy Notices » que les institutions financières doivent fournir aux consommateurs dans le cadre du Gramm-Leach Act.

77 Sur cette labellisation des sites web, lire les discussions menées par le « E-confidence Forum » créé par la Commission européenne et ses suggestions (http://www.econfidence.jrc.it)

78 Cf. pour un tel mécanisme destiné à assurer la conformité des sites web aux exigences des législations de protection des consommateurs et de sécurité, le système TRUSTMARK UK. Sur ce système, R. DE BRUIN,

79 Sur la corégulation, lire Y. POULLET, « Technologies de l'information et corégulation », in *Liber Amicorum M.Coipel,* Y. POULLET - P.WERY - P.WYNANTS, Kluwer, 2004, à paraître .

sont cependant acceptables que si elles répondent à la triple exigence de « légitimité », « conformité » et « effectivité »[80].

De telles mesures ne se substituent pas à l'obligation de fixer par la régulation publique les principes de base de la réglementation. C'est dans le cadre de ces principes que doivent être évaluées les mesures techniques[81] **et les réponses du marché aux problèmes posés par le développement des services électroniques de communication. Le constat de l'insuffisance de telles mesures ou réponses obligera le cas échéant, les autorités publiques à émettre de nouvelles réglementations (principe de subsidiarité**[82]**).**

Nous le répétons : la loi est nécessaire…. Elle oriente les initiatives auto-réglementaires et c'est à son aune que ces dernières peuvent être appréciées et jugées. Par ailleurs, rien n'est pire que l'utilisateur abandonné à lui-même, ne sachant à quelle régulation se fier, le marché ne pouvant être bon guide que s'il était transparent et le « consommateur » capable d'isoler le facteur « protection des données » des autres critères. L'User Empowerment que réaliserait certaines technologies de négociation demeure un mythe s'il n'est soumis au contrôle de la loi.

Piste de réflexion

L'appel à la co-régulation suppose la promotion de nouveaux acteurs, qui aident à la sensibilisation et offre à l'utilisateur des possibilités réelles de maîtrise de leur environnement, ainsi les certificateurs de sites web, les infomédiaires. Elle conduit à

---

[80] Sur ces trois qualités de la norme d'autorégulation, lire Y. POULLET, op.cit.: « *The **"legitimacy"** is "source oriented and underlines the question of the authors of a norm. To what extent, might the legal system accept a norm elaborated outside of the actors designated by the Constitution or under constitutional rules? This quality of the norm means that the authorities in charge of the norm promulgation must be habilitated for doing that by the community or communities of the persons which will have to respect the rule they have enacted. This legitimacy is obvious as regards the traditional State authorities acting in conformity with the competence devoted to them by the Constitution. It is less obvious when the regulation is the expression of private actors themselves as it is the case with self-regulation, particularly when it is the fact of certain obscure associations or even of private companies able to impose their technical standards.*

*The **"conformity"** is "content oriented" and designates the compliance of normative content vis a vis fundamental society values, those embedded undoubtedly in the legal texts but also beyond that those considered as ethical values to be taken into account by the legal system. Again this criterion is quite easy to satisfy and to verify in case of traditional texts issued by governmental authorities insofar these texts must be taken in consideration of already existing rules with superior values. It seems more intricate to satisfy to this criterion when the compliance with existing legislative text is not systematically checked insofar these text are not existing or not clearly identified. Indeed self-regulation is often a way to avoid the traditional and constitutionally foreseen regulatory methods of rule-making.*

*Finally, the **"effectiveness"** is "respect oriented". To what extent, a norm will be effectively respected by those to whom the norm is addressed ? So, the question about the information about the existence of the norms, about the sanctions and the way by which they might be obtained are central for determining the effectiveness of a norm. By this criterion, one means in particular the fact for the addressees of the norm to be aware of the content of the norm but also for norms to foresee a cost for its non respect by addresses who are so stimulated to follow the rule."*

[81] Comme l'écrit Dix[81] « Technology is however no panacea for privacy risks in cyberespace ; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation but a necessary additional tool"(A. DIX, "Infomediaries and Negociated Privacy Techniques", papier présenté à la *Conférence « Computers, Freedom and Privacy » (CPF 2000), 19 avril, Toronto, disponible à : http://portal.acm.org/citation)*

[82] que l'on peut exprimer comme suit : « ce que vous pouvez résoudre par l'autorégulation ou la corégulation doit l'être par ces moyens ».

promouvoir la mise au point de technologies nouvelles «sûres » et leur mise à disposition tant vis-à-vis des personnes concernées que d'intermédiaires comme les fournisseurs d'accès à Internet : les logiciels et services d'anonymisation constituent à cet égard un bel exemple.

4. Article 5 - Qualité des données

4.1. A PROPOS DU CONSENTEMENT COMME BASE DE LEGITIMITE D'UN TRAITEMENT

L'exigence de finalité légitime renvoie à une réflexion sur le **« consentement » comme fondement de la légitimité de certains traitements opérés dans le cadre de l'utilisation par la personne concernée des services de l'Internet.** Comme on le sait, même si l'article 5 se borne à mentionner le principe général de légitimité, le consentement est cité par les autorités de protection des données, la Directive européenne (article 5.1) et par la doctrine comme première base de légitimation d'un traitement. Dans la mesure où les réseaux modernes sont interactifs, le consentement peut plus facilement être réclamé comme fondement de légitimité des traitements et être préféré à d'autres fondements plus traditionnels comme la balance d'intérêts. La facilité pour le maître du fichier d'obtenir le consentement de la personne concernée explique que certaines législations n'hésitent pas à réclamer dorénavant le consentement pour légitimer certains traitements, ainsi, la Directive 2002/58 de l'Union Européenne, à propos des traitements des données de trafic, de localisation[83].

Cette considération amène certains à considérer dès lors que le consentement peut suffire pour légitimer un traitement. A cet égard, on rappelle que le développement par le World Wide Web Consortium (W.3.C.) de la Platform for Privacy Preferences (P.3.P.)[84] reposait également sur la possibilité pour l'internaute de négocier avec le fournisseur de services qui ne répondait pas à ses Privacy Preferences et d'aboutir alors à un accord qui serve de fondement légitime au traitement considéré. Même si cette négociation n'a jamais été déployée sur une grande échelle, notamment par le biais d'agent électroniques, P3P reste révélateur de la volonté de l'industrie de se donner les moyens de négocier avec la personne concernée l'utilisation qui pourrait être faite de ses données. La protection de la vie privée pourrait ainsi, dans une certaine mesure, se négocier[85].

---

[83] On mentionnera également le système de l'opt-in choisi pour régler la question de l'envoi de courrier non sollicité. Un autre argument en faveur de l'opt in est le caractère intrusif de l'envoi qui pénètre directement le domicile virtuel de la personne concernée, la facilité d'envoi de tels messages et l'absence de tout coût pour l'émetteur.

[84] Outre l'opinion émise par le Groupe de l'article 29 (Opinion 11/98 du Groupe européen de protection des données, Groupe dit de l'article 29 à propos de la Platform for Privacy Preferences (P3P) et des Open Profiling Standards (OPS),opinion disponible à http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdoes/wp11.fr.pdf),lire sur ce protocole, J. CATLETT, « Technical Standards and Privacy : An open Letter to P3P Developers », disponible à l'adresse *: http://www.junkblusters.com/standards.html*.

[85] Sur la contractualisation du traitement des données ainsi opérée par la technologie, lire P.M. SCHWARTZ, « Beyond Lessig's Code for Internet Privacy : Cyberespace, Filters, Privacy control and Fair Information Practices », *Wisconsin Law Review*, 2000, p. 749 et s. ; M. ROTENBERG, « What Larry doesn't Get the Truth », *Stan. Techn. L. Rev*., 2001,1, disponible sur le site : http://www.sth.Stanford .edu/STLR/Articles/01_STLR_1 .

Piste de réflexion

Il nous paraît cependant que le consentement ne peut constituer une base suffisante de légitimité. Il nous paraît que dans certains cas, la légitimité d'un traitement même appuyé par un consentement spécifique, informé et libre peut se voir remis en cause. Trois raisons militent en ce sens :

- **le consentement même loyalement obtenu ne peut légitimer certains traitements contraires à la dignité humaine ou à d'autres valeurs essentielles à laquelle un individu ne peut renoncer ;**
- **les individus consommateurs doivent être protégés contre des pratiques où en échange d'avantages économiques, leur consentement est sollicité ;**
- **enfin, la question de la protection de la vie privée n'est pas une simple affaire privée mais met en jeu des considérations d'ordre social et exige une possibilité d'intervention et un contrôle marginal par les autorités publiques**[86]

4.2. LE CAS PARTICULIER DU CONSENTEMENT DES MINEURS

Le consentement au traitement par des **individus mineurs relatives à des données à caractère personnel les concernant** pose des problèmes délicats. Le consentement doit émaner d'une personne capable au sens de la loi. Le consentement exprimé par un mineur ne suffit point sans l'autorisation parentale, ce qui n'empêche pas de devoir l'associer à ce consentement dans la mesure de ses capacités de compréhension voire d'exiger à côté du consentement parental son consentement exprimé de manière autonome .

Récemment, le développement de services interactifs sur Internet a donné à ses principes une actualité. Les enfants sont une des cibles privilégiées pour les « vendeurs » de tous poils présents sur Internet et nombre de méthodes de collecte d'informations sont utilisées pour les amener à fournir des informations personnelles : jeux-concours, formulaires d'adhésion, etc.

La vérification du consentement parental à la délivrance de telles informations apparaît donc nécessaire. La loi américaine, le « Children's Online Privacy Protection Act » (COPPA) de 1998[87] exige que le fournisseur de services collectant des informations auprès de mineurs soient soumis au principe du « Verifiable Parental Consent » défini comme « tout effort raisonnable (prenant en considération la technologie disponible), comprenant une demande pour l'autorisation pour la collecte, l'utilisation et la communication futures de données relatives à l'enfant, et telles que décrites dans la notice d'information, de manière à garantir que les parents d'un enfant reçoivent notification de ces pratiques de collecte, utilisation et communication et puissent autoriser la collecte, l'utilisation, la communication et ses utilisations ultérieures avant que l'information ne soit collectée auprès de l'enfant ».

Récemment, la Commission belge de protection de la vie privée[88] a émis à ce même propos un avis plus nuancé insistant sur l'autonomie de l'enfant tout en soulignant les limites de celle-ci : « *La Commission est d'avis que le consentement d'un parent ne doit pas être*

---

86 A ce propos, les réflexions de SCHWARTZ, article cité note précédente.

87 Sect. 1302(9). Le texte de la loi américaine est disponible sur le site de la Federal Trade Commission http://www.ftc.gov/ogc/coppa1.htm. Quelques exceptions à cette exigence sont prévues par la loi.

88 Avis n°38/2002 relatif à la protection de la vie privée des mineurs sur Internet, avis disponible sur le site de la Commission : http://www.privacy.fgov.be

systématiquement requis lorsque des données relatives à un mineur sont traitées sur l'Internet. Elle souligne ainsi que le consentement parental ne devrait pas être un mécanisme permettant à un parent de passer outre la décision de l'enfant, sauf s'il existe un risque sérieux que l'enfant n'apprécie pas correctement les conséquences de sa décision, ou que sa naïveté naturelle soit exploitée. C'est la raison pour laquelle la Commission insiste dans ce document sur la nécessité d'obtenir un consentement parental dans des circonstances déterminées, et notamment : lorsque l'enfant n'a pas atteint l'âge de discernement, lorsque des données à caractère sensible sont collectées, lorsque la finalité poursuivie n'est pas dans l'intérêt direct du mineur (marketing, transmission des données à des tiers), lorsque les données sont destinées à être rendues publiques (diffusion d'informations sur un forum de discussion, ou sur le site Internet d'une école) ».

4.3. A PROPOS DES TRAITEMENTS « INCOMPATIBLES »

Le principe de **« compatibilité »** des finalités exige qu'en cas de traitements dérivés, ces traitements ne heurtent pas les prévisions raisonnables de la personne concernée. L'accélération du progrès technologique, les potentialités infinies de traitements nouveaux offertes par les logiciels et les données disponibles sur le réseau justifient la nécessité de s'interroger sur cette question de la régulation des traitements ultérieurs et de leur compatibilité avec les finalités initiales d'enregistrement et sur les moyens de faire respecter le principe d'interdiction de traitements incompatibles.

Ainsi, les RFID conçus au départ par les entreprises de biens de consommation comme un outil de lutte contre les vols dans les grands magasins sont devenues un outil puissant d'analyse des comportements des consommateurs, leur profilage etc. La mise à disposition par un auteur scientifique de son curriculum vitae et de ses publications aux fins de faire connaître son œuvre peut servir à le classer politiquement ou philosophiquement. La publication des décisions jurisprudentielles dans de vastes bases de données a un but scientifique et aide à faire connaître le droit. La possibilité de recherche par le nom des parties ou le type d'affaires peut permettre de créer des listes noires (ainsi, la liste des employés ayant pris recours contre leurs employeurs ou ayant été licenciés par eux).

Piste de réflexion

La régulation qui pourrait être proposée doit tenir compte de l'intérêt que peuvent présenter les traitements ultérieurs[89] . Sans doute dans toute la mesure du possible, le consentement doit-il être demandé ou le codage voire l'anonymisation des données requises (principe de minimisation). A défaut, on devrait pouvoir admettre que le maître du fichier qui souhaite lancer un traitement ultérieur soit tenu de motiver soigneusement au regard de la balance d'intérêts la légitimité d'y procéder et tenu d'en informer les personnes concernées au moins collectivement.

---

[89] Ainsi une base de données de soins de santé peut ayant servi à une première finalité thérapeutique être utilisée par la suite à des finalités de recherche scientifique, une banque peut proposer à un moment donné un service nouveau à ses clients fondé sur une exploitation plus performante des données relatives à ses clients.

Quant aux solutions techniques[90], on peut, par exemple dans le cadre des moteurs de recherche, songer à donner à l'usager du réseau, les moyens de définir lui-même ce qu'il entend par finalités « compatibles », ainsi, les systèmes techniques « no-robot » apposés sur des pages web interdisent leur prise en compte par les engins de recherche. Autre exemple de solutions techniques : à propos de l'utilisation marketing des données collectées sur le net, des infomédiaires proposent leurs services pour sélectionner les utilisations possibles des données des internautes à des fins de marketing, etc.

4.4. A PROPOS DES UTILISATIONS DES SERVICES DE COMMUNICATION AU SEIN DE GROUPES ET DE LA LEGITIMITE DE LEURS TRAITEMENTS INTERNES AU GROUPE

L'utilisation des systèmes d'information est souvent collective, ainsi au sein d'une famille (utilisation d'un même P.C. ou d'un même terminal) ou d'une organisation (partage de ressources communes au sein d'un intranet). Par ailleurs, il peut arriver que les terminaux soient mises à la disposition d'utilisateurs par une personne qui, à ce moment-là, souscrit seul l'abonnement pour ces diverses utilisateurs (ainsi le père de famille ou le dirigeant d'entreprise qui souscrit les abonnements aux mobilophones mis à disposition de ses enfants ou de ses employés). De tels partages ou de telles mises à dispositions induisent la possibilité pour les premiers de contrôler l'utilisation faite par les personnes sous sa dépendance des terminaux mis à leur disposition. Ce contrôle peut être légitime dans la mesure où il est lié à des questions de sécurité du réseau ou de limitation des dépenses mais il peut induire également un accroissement abusif du pouvoir de surveillance des uns par rapport aux autres.

Piste de réflexion :

Nombre d'initiatives réglementaires ou d'autorégulation ont été prises pour fixer les règles et limites de la surveillance des employés par rapport à leur utilisation des ressources informationnelles mises à leur disposition. Il serait sans doute bon que le Comité consultatif examine ces règles souvent disparates et fixe, après avoir entendu les parties concernées, quelques principes communs qui permettent d'harmoniser les comportements. Au delà, il serait utile de réfléchir à la distinction entre « abonnés » et « utilisateurs » prônée par la directive 2002/58 CE qui conduit à s'interroger sur les limites du traitement par l'abonné des données de trafic et de localisation générés par les utilisateurs (par exemple en ce qui concerne la facturation) et octroie des droits spécifiques aux utilisateurs vis à vis des abonnés (ainsi le droit de restreindre l'identification de la ligne appelante ou de s'opposer aux traitements des données de trafic)

5. Article 6 - Données sensibles

Piste de réflexion

Deux catégories particulières de données devraient être ajoutées à la liste des données sensibles au vu des risques nouveaux suscités par le développement technologique

---

[90] Il s'agit ici d'une belle anticipation du principe que nous développerons dans la Partie III sous le titre : « Principe de promotion de solutions technologiques conformes au respect des exigences de protection des données ou améliorant la situation des personnes protégées par le droit ».

- **les « numéros d'identification » (avec ou sans lien avec l'identité au sens étroit) qui permettent de coupler de multiples bases de données ou données et se généralisent tant dans le secteur tant privé que public ;**

- **les « profils » définis par la loi suisse comme « une combinaison de données permettant une évaluation des aspects essentiels de la personnalité d'un individu ». L'approche suisse pourrait être étendue suivant l'exemple de la loi norvégienne au « profilage anonyme » lorsque ce profilage anonyme est utilisé pour prendre ultérieurement des décisions vis-à-vis de personnes relevant de ce profil**[91]

Par ailleurs, la définition extrêmement large des données sensibles (par ex. un nom patronymique révèle l'origine raciale ; l'achat d'un ouvrage sur le Coran sur un site web peut révéler les convictions religieuses, etc.) rend absolument nécessaire l'abandon d'une définition de la nature en soi des données et la nécessité d'une approche par la finalité : le traitement a-t-il pour finalité la révélation d'une origine raciale, etc. ? Cette approche permettrait de considérer comme sensible non une donnée mais un traitement même si aucune donnée a priori sensible n'y est contenue. Ainsi, les recherches sur Google pratiquées par un internaute de sites de voyage à Rome, son achat de livres religieux, sa lecture d'une encyclique pontificale, etc. pourraient être traitées comme révélant une opinion religieuse.

6. Article 7 – Sécurité des données

L'article envisage la sécurité dans un sens très limité : essentiellement la destruction des données et l'atteinte à la confidentialité. Il serait utile que la sécurité porte sur les 3 aspects de la sécurité au sens large « intégrité, disponibilité et confidentialité » et que soient repris les 9 principes directeurs de l'OCDE pour la sécurité des systèmes d'information établis en 1992 (principes de responsabilité, de sensibilisation, d'éthique, de multidisciplinarité, de proportionnalité, d'intégration, d'adaptation, de réévaluation, de démocratie).

Par ailleurs, l'absence de sécurité du réseau et la multiplication des agissements illicites possibles rendent nécessaires l'obligation des fournisseurs de services de communications électroniques de prévenir les utilisateurs du réseau, des risques liés à l'utilisation de leur service.

Enfin, on insistera sur l'importance de l'autorégulation en la matière : développement de normes en la matière ; méthodes d'audit ; systèmes d'agrément de S.I., etc. La sécurité organisationnelle et technique des systèmes d'information doit devenir partie intégrante de la politique de protection des données.

Piste de réflexion

Les organes de normalisation développent ces dernières années des tentatives de normalisation technique et organisationnelle de la sécurité et de la protection des données[92]**. Ces divers efforts doivent être suivis et encouragés par le Comité consultatif.**

---

[91] Sur ce point, L .BYGRAEVE, *Data Protection Law*, Inf. Law Series, Kluwer Law Int., Den Haag, p. 330 et s.

[92] Ainsi les travaux de l' ISO/IEC/ITU/UN ECE MoU Management Group and Privacy Technology Standards et les décisions récentes (Berlin 25-29 oct.2004) de l'ISO/IEC JTC 1/SC 27 : « Information Technology-Security Techniques) de supporter le développement de « Privacy Technologies Standards » (Résolution 15) et de lancer un projet d'évaluation et de test des PETS (projet PETTEP) (Résolution 18)

A propos de sécurité, on note les exigences de confidentialité des communications au sens large. Ces exigences se comprennent par le fait que désormais la technologie interactive du réseau permet à la personne utilisatrice de cette technologie de communiquer avec les autres personnes connectées au réseau et ce pour des finalités personnelles. Ceci explique que le principe du secret des correspondances et de l'interdiction des écoutes doit désormais s'étendre à l'ensemble des communications électroniques, à la fois dans leurs contenus et leur existence. Par ailleurs, ils soulèvent la question du statut des entreprises acheminant les messages ou intervenant dans cet acheminement, ne faut-il pas à l'instar des réglementations relatives aux postes et aux opérateurs traditionnels des réseaux téléphoniques, soumettre ces entreprises à une réglementation qui garantissent une telle confidentialité ?

7. Article 8 – Garanties complémentaires pour la personne concernée

Sans doute est-ce sur ce point que nombre de suggestions et recommandations pourraient être proposées par le Comité consultatif. Il s'agit de proposer une amélioration de la situation des personnes concernées afin de leur assurer la possibilité d'une « autodétermination informationnelle » au moment où, comme nous l'avons montré dans la première partie, cette maîtrise tend à diminuer au vu de la double opacité à la fois du fonctionnement des terminaux et du réseau. Nous plaidons dans la troisième partie pour la reconnaissance de droits nouveaux, indispensable corollaire de la perte de contrôle par les utilisateurs des systèmes d'information de leur maîtrise de l'environnement informationnel. Ainsi, nous souhaitons voir consacrer à tout le moins :

1. d'un droit de la personne concernée à la **réciprocité des avantages** ;
2. du droit de la personne concernée qui utilise des **équipements terminaux à disposer d'équipements au fonctionnement transparent** et réduisant autant que faire se peut des agissements illicites .

On y ajoutera sans doute :

3. la reconnaissance du droit de la personne concernée à comprendre la **logique des décisions** qui lui sont appliquées sur base d'un raisonnement automatisé.
4. le devoir de « pédagogie législative » des fournisseurs de services de communications électroniques vis à vis de leurs clients. Il s'agit pour eux de rappeler les principes de la Convention à ceux qui souhaitent utiliser la connexion pour offrir des services d'accès à des banques de données ou créer des traitements à partir des services offerts et en toute hypothèse de prévenir tout utilisateur des risques liés à leur utilisation du Net.

8. Article 9 – Exceptions et restrictions

Une exception générale devrait être ajoutée, selon nombre d'auteurs, en ce qui concerne les traitements de données à caractère personnel à « but familial ou domestique ».le raisonnement est juste : on ne peut au nom de la protection des données d'autrui violer l'intimité de celui qui traite des données pour son propre compte. La portée de cette exception doit cependant tenir compte comme le montre l'affaire Linqvist déjà citée du fait que des réflexions privées postées sur un site web sortent indéniablement de la sphère privée ou domestique des intéressés et rendues accessibles à un nombre indéterminé et illimité de personnes.

Le point 2 devrait prévoir des exceptions liées à la nécessité de garantir la liberté d'expression ou d'opinion (principe du juste équilibre entre la protection des données et la liberté d'opinion et/ou d'expression).

Le point 3 à propos des statistiques ou recherches n'envisage que les risques liés à la protection des données individuelles à la base de la recherche ou de la statistique.

Comme nous l'avons souligné, la statistique et la recherche scientifique nécessitent certaines précautions même lorsqu'elles travaillent sur des données anonymes ou rendues anonymes dans la mesure où elles introduisent la possibilité d'appliquer les profils ainsi créés à des individus[93].

9. Article 12 - Flux transfrontières de données et article 2 du protocole additionnel (signé le 8 novembre 2001)

L'article 2 du protocole additionnel adopte le concept de « protection adéquate » comme critère pour l'acceptation d'un flux transfrontières. On suppose que cette référence également utilisée par la directive européenne emporte l'adhésion par le Conseil de l'Europe aux multiples documents d'interprétation de ce concept développé depuis la directive par les autorités européennes compétentes (Groupe de l'article 29 et décisions de la Commission sur le caractère adéquat[94]). Sans doute serait-il utile d'ajouter que la détermination du caractère adéquat suppose une interprétation évolutive dans la mesure où l'adéquation se constate non point une fois pour toutes mais en fonction des interprétations données à la Convention par la jurisprudence de la Cour de Strasbourg et des réglementations nouvelles prises (recommandations, protocoles additionnels).

De même pour les deux dérogations et en particulier la seconde relative aux garanties jugées suffisantes, il est sans doute fait référence aux exceptions proposées par la directive 95/46 et à l'interprétation donnée depuis à ces exceptions (décisions en matière de clauses contractuelles et à propos des règles obligatoires en matière de flux à l'intérieur de groupes d'entreprises). L'existence de différents hypothèses qui permettent de légitimer les flux transfrontières entraîne, nous semble t'il, l'obligation de proposer une grille permettant de comprendre la hiérarchie et la cohérence de ces différentes hypothèses et les cas de figure où chacune de ces hypothèses s'applique.

Pistes de réflexion

Les flux transfrontières soulèvent quelques questions non abordées par la Convention mais qui serait utilement traitées par le Comité consultatif :

1. **Ne faut-il pas adopter des critères de localisation des traitements sur le web ?**

---

93 Cf. notre commentaire à propos de l'article 1 (supra 5.1.)

94 Cf. les nombreuses opinions émises par le Groupe dit de l'article 29 à cet égard et en particulier le document de travail n° 12 du 24 juillet 1998 relatif au transfert de données vers des pays tiers : application des articles 25 et 26 de la Directive 95/47 relative à la protection des données (disponible sur le site http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp1998/wpdocs98_fr.htm) et l'étude de B. HAVELANGE et Y. POULLET, « *Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel* », Annexe au Rapport annuel du Groupe de l'article 29 de la Directive 95/46/CE, Office des publications officielles des Communautés européennes, Luxembourg, 1998.

2. **Qu'est-ce qu'un flux transfrontières ? Ne faut-il pas distinguer les flux impliquant un transfert actif des données et ceux impliquant un transfert passif c'est à dire entièrement sous le contrôle du maître du fichier localisé à l'étranger(ex. extraction automatique de certaines données dans une base de données d'une filiale d'une multinationale) ? Ne faut-il pas en matière de services atteignables via le Net parler de flux transfrontières potentiels ?**

3. **Le principe d'interdiction des flux transfrontières souffre diverses exceptions : la « protection adéquate » offerte par les normes externes au maître du fichier en vigueur dans l'Etat considéré, le contrat passé entre les maîtres du fichier importateur et exportateur, les règles internes que le maître du fichier ou les maîtres s'imposent au sein d'un groupe d'entreprises, enfin quelques cas particuliers liés à la nature du flux considéré. La question soulevée par nombre de maîtres de fichier est de pouvoir identifier facilement quel type d'exceptions s'applique dans son cas particulier. En d'autres termes, qu'une systématique permettant de mieux à quels types de flux s'applique chaque catégorie d'exception soit proposée et que sur base de cette systématique, une interprétation du champ d'application de chaque exception puisse être proposée.**

4. **Ne faut-il pas esquisser quelques éléments de droit et de juridiction applicables en cas de flux transfrontières ?**

5. **Comment réglementer l'accès à partir de l'étranger à des données localisées en Europe (cas des autorités américaines vis à vis des données relatives aux passagers de voyages aériens (P.N.R.) ou à des flux en provenance et à destination de pays membres mais captés lors de leur transit par des réseaux internationaux ou étrangers (cas ECHELON) ?**

6. **Enfin, se pose la question de l'effectivité des décisions prises au nom de la souveraineté des pays membres du Conseil de l'Europe au nom de la défense des droits de l'Homme ? Comment garantir celle-ci ? Doit-on suivre la suggestion d'obliger les fournisseurs de services de communications électroniques à se localiser sur le territoire d'un Etat membre ?**

10. Conclusion de la partie II

Les principes énumérés par la Convention n° 108 offrent grâce à la souplesse de leur contenu des solutions en grande partie satisfaisantes pour garantir une protection appropriée des personnes concernées, utilisatrices des réseaux et systèmes d'information, à condition, certes, que certains de ses concepts et règles soient l'objet de réflexions à propos de leur signification dans un contexte, notamment technologique qui n'est plus celui dans le cadre duquel ces principes ont été élaborés. Une interprétation évolutive de la notion d'identité, de maître du fichier a été suggérée, de même les dispositions relatives à la légitimité des traitements prennent dans le contexte de réseaux interactifs, internationaux et coopératifs obligent à s'interroger sur la portée et les limites du consentement, la compatibilité des traitements et leur sécurité et, enfin, sur la question omniprésente des flux transfrontières.

La prise en considération de deux textes importants publiés depuis la Convention et que nous avons d'emblée souhaité prendre en compte dans l'analyse de l'évolution des principes de la Convention permet cependant de pointer quelques compléments réglementaires nécessaires pour répondre aux défis posés à la protection des données par les développements technologiques liés à l'Internet et ce sur des questions non abordées par la Convention mais

qui apparaissent être une réponse particulièrement utile aux risques nouveaux soulignés dans la première partie de notre étude.

Ainsi, la recommandation n° R(99) 5 du Comité des Ministres relative à la protection des données sur l'Internet évoque l'importance de l'anonymat des personnes concernées : « *L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée ...* »[95]. Cette revendication d'un « droit à l'anonymat » apparaît relayée par d'autres textes européens. Par ailleurs, la recommandation attire l'attention dans la partie III sur les devoirs des « *fournisseurs de services d'Internet »,* notion que le Point IV élargit à toute une série d'acteurs « *tels que fournisseurs d'accès, de contenus, de réseau, les concepteurs de logiciels de navigation, les coordinateurs de forums ou d'info-kiosques »... « de tout type d'info-routes ».* Cette volonté de prescrire à destination de ces acteurs nouveaux, nés du développement de nos réseaux interactifs, des charges spécifiques se retrouve déjà dans les réflexions abordées ci dessus à propos des données de trafic et de localisation mais elles ne s'arrêtent pas là.

En particulier, la directive 2002/58/CE dite « vie privée et communications électroniques » pointe le rôle particulier de deux acteurs :

- Les opérateurs de réseaux (en ce compris les fournisseurs d'accès à Internet), c'est à dire ceux qui fournissent « *des systèmes de transmission et le cas échéant, les équipements de communication ou de routage et les autres ressources qui permettent l'acheminement de signaux*[96] » qui constituent des interfaces obligés entre l'utilisateur du réseau en tant que personne concernée et les multiples acteurs de l'Internet qui pourront traiter les données multiples générées consciemment ou non par l'utilisation du réseau. C'est à eux qu'incombent certains devoirs, tels celui de prévenir des risques liées à l'utilisation du réseau, de garantir la sécurité de ses services, de permettre des restrictions à l'identification de la ligne appelante, etc. ;

- les fournisseurs d'équipements terminaux, en particulier -mais non uniquement-, des logiciels de navigation, dont les caractéristiques techniques doivent mettre en œuvre les dispositions de la directive. En particulier, la Directive prévoit la possibilité d'imposer certains « *mesures afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel ».*

En d'autres termes, les textes précités plaident au delà des dispositions de la Convention pour trois interventions : la première est le « droit à l'anonymat » ; la deuxième, une réglementation des « produits terminaux »[97] ; la troisième exige la définition d'un statut et d'obligations particulières pour les fournisseurs de services de communication intervenant de manière nécessaire dans l'acheminement des messages. Ces interventions complémentaires se

---

95 Point II.3 de la Recommandation, lire aussi le point II.2, II.4, III.4.

96 Directive 2002/21/CE, article 1(d)

97 à comprendre au sens de la Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, JOCE n° L 091 du 07/04/1999 pp. 0010 – 0028, c-à-d *comme un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications (à savoir des réseaux de télécommunications servant entièrement ou en partie à la fourniture de services de télécommunications accessibles au public).*

justifient, comme nous l'avons dit, par les risques nouveaux dus aux modifications du paysage technologique, à savoir la perte de contrôle constatée dans le chef de la personne concernée du fait d'un double interface non maîtrisée : d'une part, les terminaux dont le fonctionnement est opaque et d'autre part, les intermédiaires techniques qui interviennent entre l'utilisateur du réseau et le destinataire de la communication.

Pour fonder d'avantage encore ces trois revendications, notre troisième partie identifie et explicite, à partir de textes récents nationaux ou internationaux, quelques nouvelles facettes de la protection des données, impliquées par la volonté de rendre à la personne concernée une certaine maîtrise de son environnement et de la circulation de son image informationnelle.

III. QUELQUES NOUVEAUX PRINCIPES POUR FAVORISER L'AUTODETERMINATION INFORMATIONNELLE DANS L'ENVIRONNEMENT TECHNOLOGIQUE NOUVEAU

Les caractéristiques même de l'environnement des services de communication électronique (omniprésence, complexité, opacité, performance et polyvalence) et des terminaux (interactivité, dimension internationale des réseaux et services et producteurs d'équipement, opacité de fonctionnement) créent de nouveaux risques et aggravent les risques d'atteinte aux libertés individuelles et à la dignité humaine.

La parade à ces risques n'est possible que par la consécration de principes nouveaux améliorant la protection des personnes concernées et lui donnant une meilleure maîtrise de son environnement. Ce n'est en effet que dans la mesure où cette maîtrise est possible, que la personne concernée pourra prendre effectivement la responsabilité de sa propre protection et mieux disposer des moyens d'une véritable autodétermination informationnelle.

La formulation de ces nouveaux principes est une première tentative. Elle s'appuie sur des textes souvent disparates que nous avons essayé de structurer suivant cinq principes, n'osant pas à ce stade ici parler de « droits » nouveaux de la personne concernée. A la fois leur énoncé, leur contenu et leur extension sont soumises à la discussion du Comité Consultatif qui pourrait sur base de cette discussion prendre le cas échéant les recommandations ou autres mesures ad hoc pour mieux les consacrer.

1. Premier principe : Le chiffrement et de l'anonymat « réversible »

Le chiffrement des messages assure la protection de l'accès au contenu des communications. Leur qualité varie et les techniques de chiffrement et de déchiffrement peuvent également être diverses. Les logiciels d'encryptage placés sur l'ordinateur de l'internaute (par exemple, SSL ou PGP) sont désormais accessibles à des prix abordables et généralement intégrés dans les logiciels grand public. La notion d'anonymat quant à elle devrait sans doute être redéfinie et, dans la foulée, d'autres termes comme « pseudonyme » ou « non identifiabilité » devraient être préférés dans la mesure où cette notion d'anonymat demeure ambiguë. Ce qui est recherché est bien souvent, non un anonymat absolu, mais une « **non identifiabilité » fonctionnelle de l'auteur d'un message vis-à-vis de certaines personnes**[98]. Nombre de textes à caractère non contraignant préconisent le « droit » du citoyen[99] à disposer de l'anonymat lorsqu'il utilise les services offerts par les technologies nouvelles. La Recommandation n° R(99) 5 du Comité des Ministres du Conseil de l'Europe[100]

---

98 Sur ce point, lire J. GRIJPINK et C. PRINS, "Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions ?", 17 *CL&SR* (2001), p. 378 et ss.

99 A ce propos, lire notamment S. RODOTA, "Beyond the E.U. Directive : Directions for the Future", in *Privacy : New Risks and opportunities*, Y. POULLET- C. DE TERWANGNE et P. TURNER (ed.), Cahier du CRID, n° 13, p. 211 et ss.

100 Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes », texte disponible sur le site du Conseil de l' Europe. Dans le même sens, la recommandation 3/97 du groupe dit de l'article 29 intitulée : « l'anonymat sur Internet ». Cf. également l' avis de la Commission belge de la vie privée pris d'initiative sur le commerce électronique (Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission belge de la vie privée :

énonce, nous le rappelons, le même principe: « *L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée*. » et souligne à ce propos l'intérêt des « Privacy Enhancing Technologies » disponibles sur le marché.

Piste de réflexion

Celui qui utilise les moyens modernes de communication devrait avoir le choix de rester non identifiable au regard, tantôt de tiers intervenant dans l'acheminement du message ou de prestataires intervenant dans cette chaîne de communication, tantôt du ou des destinataires de la communication et disposer gratuitement, ou au moins à des prix abordables, des moyens d'exercer son choix[101]. **La mise à disposition à des coûts abordables de moyens ou de services de chiffrement et d'anonymisation est une condition nécessaire à une responsabilisation de l'internaute.**

L'anonymat ou la « non identifiabilité fonctionnelle» requis ne sont cependant pas absolus. Au droit à l'anonymat des citoyens, s'oppose l'intérêt supérieur de l'Etat qui pourra imposer des limitations lorsque celles-ci constituent des mesures nécessaires « *pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique la prévention, la recherche, la détection et la poursuite de (certaines) infractions pénales* ». L'équilibre entre le légitime contrôle des infractions et la protection des données pourrait être trouvé dans des systèmes de « pseudo-identité » attribuée à un individu par un fournisseur de service spécialisé auprès duquel dans les seuls cas prévus par la loi et moyennant les modalités fixées par celle-ci pourrait s'opérer le lien entre l'identité réelle d'un usage et son pseudonyme.

Piste de réflexion

Au-delà, d'autres solutions pourraient être imposées par une réglementation des appareils terminaux : suppression du « bavardage » des navigateurs, la création d'adresses éphémères ou relatives à un groupe d'individus et une différenciation des données d'adressage suivant les tiers qui auront accès aux données de trafic ou de localisation et la disparition des pointeurs (Global Unique Identifiers) par l'uniformisation des protocoles d'adressage.

Enfin, le statut des « anonymisers », véritable tiers de confiance pour celui qui y fait appel, devrait être réglementé afin d'offrir, à celui qui y recourt certaines garanties quant à la qualité des services offerts, et à l'Etat, la garantie de pouvoir techniquement accéder au contenu des télécommunications, dans les conditions prévues par la loi[102]..

---

http://www.privacy.fgov.be) rappelle à bon escient qu'il existe des mécanismes qui permettent d'authentifier l'émetteur d'un message sans nécessairement l'obliger à s'identifier.

[101] Cf. à cet égard, la recommandation de la CNIL suivant laquelle tout accès à un site marchand doit être possible sans que l'internaute n'ait à s'identifier préalablement (M. GEORGES, Relevons les défis de la protection des données à caractère personnel : l' Internet et la CNIL, in *Commerce électronique- Marketing et vie privée*, Paris, 2000, p.71 et 72.

[102] La qualité des services offerts et des exigences de confidentialité pourraient être l'objet d'un cahier des charges, comme il en est proposé en matière de signatures électroniques. L'agréation d'un « anonymiser » reconnaîtrait son respect du cahier des charges. On peut concevoir que l'agréation ne soit pas requise mais volontaire, équivalent dans ce cas à un label de qualité. .

2. Deuxième principe : La réciprocité des avantages

Ce principe pourrait s'exprimer comme suit : le législateur entend, chaque fois, que cela est possible, mettre à charge de celui, qui utilise la technologie aux fins de développer ses activités professionnelles, certaines obligations supplémentaires qui permettent de rétablir l'équilibre traditionnel des parties en présence. La justification du principe est simple, si la technologie accroît les capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d'opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concernée, l'administré, le consommateur, bref le fiché, puisse bénéficier, dans une proportion comparable, des avantages de cette technologie.

Quelques dispositions récentes se fondent sur l'exigence de la réciprocité des avantages pour obliger celui qui utilise des technologies à mettre à disposition de l'internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits qui peuvent être mis à mal par l'utilisation de ces moyens électroniques.

Citons ainsi, la directive européenne 2001/31/CE sur les services de la société de l'information, la possibilité de s'opposer via des moyens électroniques au spamming. L'article 5.3 de la directive 2002/58 « Vie privée et communications électroniques » exige de même que toute « *utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou utilisateur faire l'objet d'une information de ce dernier et que celui-ci dispose du droit de refuser un tel traitement …* ». La possibilité pour l'abonné (article 8.1.) de restreindre « *par un moyen simple et gratuit l'identification de la ligne appelante et ce appel par appel…et ce pour chaque ligne* » en est une autre manifestation, riche d'applications possibles si la notion de ligne appelante est étendue aux diverses applications de l'Internet (ainsi, les services du web, de courrier électronique)[103]. Cette possibilité conduit à une obligation corrélative pour le fournisseur du service de permettre au destinataire soit de refuser les appels entrants non identifiés, soit d'empêcher leur identification (article 8.2 et 8.3).

Vis à vis des administrations, le droit à la transparence consacré par les législations de type « Freedom of Information Act » ajoute encore quelques obligations d'information à charge de l'administration vis à vis du citoyen. Au Royaume-Uni, il convient de saluer l'apparition récente d'une garantie de bonne gestion des données à caractère personnel par les services publics[104]. Récemment, une commission suédoise[105] a recommandé l'adoption d'une législation qui garantit le droit pour le citoyen de suivre électroniquement l'avancement de son dossier depuis la naissance de celui-ci jusque et y compris son archivage et l'obligation pour l'administration d'adopter une « *good public access structure* » permettant à l'individu de retrouver et de localiser

---

[103] A noter le lien entre ces dispositions et le principe de l'anonymat.

[104] *« A Public Service Guarantee For Data Handling : A public service guarantee for data handling is now available for implementation in public bodies. This sets out people's rights about how their personal data is handled by public authorities and the standards they can expect public organisations to adhere to »*

http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2

[105] P. SEIPEL, "Information System Quality as a Legal Concern", in *Information Quality Regulation : Foundations, Perspectives and Applications*, U.GASSER (ed.), Nomos Verlagsgesellschaft, 2004, p. 248. Cf également le rapport de la Commission suédoise publié sous la responsabilité de P. SEIPEL, *Law and Information Technology : Swedish Views*, Swedish Government Official Reports, SOU 2002, 112.

plus facilement un document spécifique. Une proposition de loi proposerait même que les documents officiels qui soient à la base d'une décision puissent d'une manière ou l'autre être liés aux autres documents relatifs au cas. A une administration plus efficace grâce à la technologie, doit répondre une administration plus transparente et plus accessible pour les citoyens. L'accès du citoyen s'entend non seulement des données le concernant mais également des textes réglementaires qui ont déterminé la décision de l'administration.

Pistes de réflexion

En matière de protection des données, on peut de même envisager que certains droits de la personne concernée, ainsi le droit à l'information, le droit d'accès et de rectification et le droit de recours puissent demain se réaliser par des moyens électroniques. De multiples applications de ce droit peuvent dès maintenant être suggérées :

1. **le droit à l'information de la personne concernée doit pouvoir s'opérer à tout moment par un simple clic (ou plus largement par un simple geste positif, électronique et immédiat) sur un sigle permettant l'accès à une « Privacy Policy » dont on peut espérer qu'elle soit d'autant plus précise et complète que le coût de la diffusion est réduit dans le cas de l'utilisation du media électronique. Cette démarche doit rester anonyme pour le serveur de la page (crainte de « fichage » des internautes « privacy concerned »). Au delà, en cas de labellisation du site, on peut songer à rendre obligatoire l'existence d'un hyperlien qui permettrait à partir du sigle du label de visiter la page du site de l'organe de labellisation relative au site web en question. Même suggestion à propos de la déclaration d'un maître du fichier à l'autorité de contrôle, un hyperlien serait ainsi placé sur une page incontournable du site web, objet du traitement déclaré et la page du site de l'autorité de contrôle reprenant la déclaration du site concerné ;**

2. **le droit d'accès de la personne concernée doit demain pouvoir s'exercer via le media électronique sur base de l'utilisation de la signature électronique. Il devrait obliger la personne responsable à structurer ses fichiers de manière à permettre à la personne d'exercer de façon aisée ce droit d'accès. Des renseignements complémentaires comme l'origine des données, la liste des tiers à qui communication de certaines données a été faite devraient être systématiques.**

   Au delà, nous avons noté[106] que de plus en plus dans les vastes réseaux publics et privés, la donnée à caractère personnel n'était plus collectée pour une ou des finalités précises mais « déposées » à un endroit du réseau pour servir à des finalités définies de manière évolutive en fonction des capacités de traitement nouvelles ou de besoins non aperçus au départ. Face à cette réalité, il importe que la personne concernée puisse obtenir une documentation décrivant les flux au sein du réseau, les données en question et les divers utilisateurs, bref ce qu'on peut appeler un «cadastre des flux»[107] ;

---

[106] Partie II, commentaire de l'article

[107] Cette idée a été reprise par deux lois belges récentes qui obligent un comité sectoriel à établir pour le réseau en lien avec le Registre National (Loi du 8 août 1983 organisant un registre national des personnes physiques modifié par la loi du 25 mars 2003, M.B. 28 mars 2003, art.12 § 1) et celui en lien avec la Banque Carrefour des entreprises (Loi 16 janvier 2003 portant création d' une Banque Carrefour des entreprises, M.B. 5 fév. 2003, article 19 § 4).

3. **les droits de rectification et/ou d'opposition devraient pouvoir s'opposer en ligne auprès d'une personne désignée chargée de l'examen de plaintes ou de gérer la liste des oppositions et dont le statut pourrait être défini ;**

4. **le droit de recours, également, ne mériterait-il pas de pouvoir bénéficier des avantages que représente la cybermagistrature, saisine on-line, gestion de l'échange par voie électronique des arguments des deux parties et finalement prononcé de la décision ou de la proposition de médiation ?**

5. **le droit lorsqu'une décision soit automatisée, soit signifiée par le biais d'un réseau est opposée à la personne concernée (ainsi, refus d'un permis de bâtir suite à une procédure dite de téléadministration) de pouvoir connaître par le même canal la logique suivie pour la prise de décision. A cet égard, en matière de service public[108], le citoyen devrait pouvoir bénéficier du droit de pouvoir tester de manière anonyme les logiciels d'aide à la décision ou systèmes expert qui pourront lui être appliqués le cas échéant (ainsi, un logiciel d'aide au calcul automatique des impôts ou des primes susceptibles d'être obtenues en matière de réhabilitation d'un logement).**

3. Troisième principe : La promotion de solutions technologiques conformes au respect des principes de protection des données ou améliorant la situation des personnes protégées par le droit

La Recommandation 1/99 du 23 février 1999[109], émise par le Groupe dit de l'article 29 sur base d'une analyse des risques créés pour la vie privée par les logiciels et matériels utilisés pour la communication via Internet, émet le principe suivant lequel l'industrie du logiciel et du matériel se devait de développer des produits en conformité avec les dispositions des directives en matière de protection des données personnelles. Ce troisième principe conduit à reconnaître aux régulateurs diverses modalités d'intervention.

Ainsi, il s'agit pour lui de pouvoir intervenir en cas de développements technologiques présentant des risques majeurs. Ce **principe dit de « précaution »** largement connu en droit de l'environnement[110] pourrait trouver à s'appliquer en matière de protection des données. Au nom de ce principe de précaution, il apparaît d'ailleurs comme nécessaire que les équipements terminaux de télécommunication (en ce compris les logiciels qui les animent) adoptent le paramétrage par défaut le plus protecteur possible, de manière à ce que la personne concernée ne puissent pas, par défaut, être exposée à divers risques qu'elle ignore ou qu'elle ne sait mesurer.

Par ailleurs, au nom de principe de réciprocité des avantages, il paraît opportun et non déraisonnable de doter ces équipements terminaux de télécommunications de « journaux de

---

[108] Pour les décideurs privés, le principe est le même sous réserve des intérêts légitimes du maître du fichier (en particulier, le secret des affaires qui pourrait atténuer le devoir d'expliciter la logique suivie).

[109] Recommandation sur les traitements invisibles et automatiques de données à caractère personnel sur Internet réalisés par des logiciels et matériels

[110] Sans doute, serait-il utile de développer la comparaison entre les modes de régulation de ces deux problématiques: la privacy, d'une part et l'environnement, d'autre part vu les similarités des contextes: caractère transnational des enjeux, dimension technologique importante et la similarité des approches : auto ou co-régulation du secteur, droit à l'information des personnes concernées, principe de sécurité, …

bord », à l'instar de ce qui se fait pour les logiciels de type « serveur » déployés par les entreprises et les administrations en ligne. Ceci permettrait à chaque utilisateur d'apprécier et de contrôler les personnes qui ont eu accès à son équipement et, le cas échéant, de visualiser les caractéristiques essentielles du transfert d'information qui a eu lieu.

Une disposition de la directive européenne « vie privée et communications électroniques » déjà citée, l'illustre. L'article 14 prévoit qu'en cas de non conformité d'un équipement terminal aux règles de protection des données, la commission peut prendre des initiatives en matière de standardisation de ceux-ci. En d'autres termes, la normalisation technique des équipements terminaux constitue une mesure – certes subsidiaire – d'assurer la protection des données à caractère personnel contre les risques de certains traitements abusifs, risques créés par les choix technologiques. Au delà, au nom du principe de sécurité, prescrit par l'article 7 de la Convention n°108 du Conseil de l'Europe, il s'agit d'interdire les « Privacy Killing Technologies »[111]. L'obligation de prévoir des mesures techniques et organisationnelles appropriées aux risques engendrés pour la protection des données conduira le responsable d'un site à veiller à la confidentialité des messages échangés, à signaler clairement les transmissions de données - fussent-elles automatiques et par hyperlien comme c'est le cas avec les sociétés de cybermarketing - et à lui donner les moyens aisés de les bloquer

Cette même obligation de sécurité a pour conséquence d'imposer à celui qui traite des données à caractère personnel le choix de solutions technologiques apte à minimiser voire à réduire à néant les risques d'atteinte à la vie privée. L'influence de ce prescrit sur le design des cartes à puce en particulier les cartes multifonctionnelles[112], comme les cartes d'identité, est évident.

La structuration des fichiers de santé en différents niveaux recommandée par le Conseil de l'Europe est un autre exemple de la portée de ce principe qui doit conduire à l'adoption de normes dans la conception des systèmes d'information.

Piste de réflexion

Peut-on aller plus loin et recommander le développement de « Privacy Enhancing Technologies », c'est à dire d'outils ou de systèmes qui permettent de mieux assurer le respect des droits de la personne concernée ? Il est certain que c'est le marché qui, librement, développera ces technologies mais la promotion de telles solutions « privacy compliant » ou « privacy enhancing » exige un rôle actif de l'Etat, celui de veiller par des subsides à la recherche au développement de ces solutions ; celui de mise en place de systèmes volontaires de certification ou d'accréditation des solutions élaborées et d'assurer la publicité de ces « labels » ; celui, enfin, de mettre à disposition à des coûts « abordables » les solutions technologiques considérées comme nécessaire à la protection des données.

---

[111] Selon l'expression d'un des auteurs, dans **Law and Technology Convergence in the Data Protection Field ?** *Electronic threats on personal data and electronic data protection on the Internet* in E-commerce law and practice in Europe, Ed Ian WALDEN & Julia HORNLE, under the auspices of the Eclip Network, Wood Head Publishing Limited, Cambridge, April 2001

[112] Voir à ce sujet, Jean-Marc DINANT and Ewout KEULEERS, Part 1 : « Data protection : multi-application smart cards. The use of global unique identifiers for cross-profiling purposes**".** Part 2 : " Towards a privacy enhancing smart card engineering", in *Computer **Law and Security Report***, Vol. 20, n°1, 2004, pp. 22-28, Elsevier, Oxford, 2004.

4. Quatrième principe : La maîtrise par l'utilisateur du fonctionnement des équipements terminaux

La justification du principe est patente. Dans la mesure où ces terminaux permettent à autrui de capter nos comportements, nos actions ou simplement de nous localiser, leur fonctionnement doit être transparent et sous notre contrôle. L'article 5.3. de la directive 2002/58/CE déjà citée en est une première illustration. La personne doit être clairement informée de toute utilisation à distance de son terminal (cookies, spyware) et pouvoir facilement et gratuitement s'y opposer. La règle posée par la directive 2002/58/CE qui permet à l'utilisateur d'une ligne appelante ou connectée de pouvoir empêcher la présentation de l'identification de la ligne appelante ou appelée constitue une autre illustration du principe.

Au-delà de ces exemples, on pose **le principe que tout équipement terminal devrait être paramétré de telle manière que son possesseur ou utilisateur puisse être informé de manière complète des flux entrants et sortants et puisse agir en connaissance de cause, s'il l'estime nécessaire.**

De même, la possession d'une carte à puce devrait être accompagnée, comme le prévoient certaines législations sur les cartes d'identité électronique d'une possibilité d'accès en lecture des données inscrites sur la carte, par la personne concernée.

La maîtrise suppose également que la personne puisse à tout moment décider de désactiver définitivement le terminal. En matière de RFID, la question est importante. La personne concernée doit pouvoir, gratuitement et facilement, auprès de tiers fiables[113] s'assurer de la désactivation de ce moyen technique de repérage à distance.

On note que l'usager devra pouvoir opposer ce principe à des entreprises non nécessairement visées par les réglementations classiques de protection des données dans la mesure où elles ne sont point responsables de traitement : ainsi les fournisseurs d'équipements terminaux et des multiples logiciels en particulier de navigation susceptibles d'être incorporés au terminal pour faciliter la réception, le traitement ou l'émission de communications électroniques.

Au-delà, il s'adresse aux organes de normalisation tant publics que privés qui s'occupent ou se préoccupent de la configuration de ces équipements.

L'idée essentielle est que les produits mis à la disposition des usagers des services de communications électroniques ne puissent permettre de par leur configuration même des agissements illicites, qu'ils soient le fait de tiers ou du producteur lui-même. Quelques exemples illustrent l'importance du propos :

- la comparaison des navigateurs présents sur le marché démontre que le bavardage de certains d'entre eux va bien au-delà de ce qui est strictement nécessaire à l'établissement de la communication[114].

---

[113] On songe bien évidemment à des systèmes de labellisation comme ceux décrits, supra Partie II, article 4 à propos de systèmes de co-régulation ou à des agréments donnés par l'autorité publique à certaines entreprises (régulation publique)

[114] A ce sujet, Jean-Marc Dinant , « **Le visiteur visité,** *Quand les éditeurs de logiciel Internet passent subrepticement à travers les mailles du filet juridique »,* in *Lex Electronica*, vol. 6, n°2, hiver 2001

- le traitement de la réception, de la suppression et du blocage d'envoi des cookies diffère d'un navigateur à l'autre. Ainsi, suivant les programmes de navigation et leur configuration, des traitements déloyaux seront plus ou moins faciles ; le blocage des fenêtre « popup » ou de l'envoi systématique des références des articles lu en ligne ou des mots-clés frappés sur les moteurs de recherche ne semble tout simplement pas possible ou, en tous cas, pas possible de manière simple sur le navigateur installé par défaut sur la plupart des centaines de millions d'ordinateurs personnels.
- l'utilisation d'identifiants globaux uniques (GUID) » ou de logiciels espions est également à signaler.

Pistes de réflexion

Par ailleurs, on s'interroge sur la nécessité d'équipements terminaux transparents dans leur fonctionnement permettant à leur usager d'avoir la pleine maîtrise des données envoyées et reçues. Ainsi, l'usager devrait pouvoir connaître de manière conviviale l'étendue exacte du bavardage de son ordinateur, les informations transmises et reçues, leur finalité et leur émetteur ou leur destinataire. A cette fin le journal de bord apparaît comme une technique appropriée et relative aisée à mettre en œuvre.

Au delà de ce droit de l'utilisateur d'être informé des flux entrants, on peut s'interroger sur le droit de la personne de soumettre à autorisation le fait pour un tiers de pénétrer son « domicile virtuel ». Il convient ici de rappeler les dispositions de la Convention du Conseil de l'Europe concernant la Cybercriminalité et notamment ses articles deux[115] (accès illégal) et trois[116] (Interception illégale). On remarquera ici que l'identification ou l'identifiabilité des personnes participant à une télécommunication ne constitue pas une condition d'application de cette Convention. Semblablement, l'accès non autorisé à un système informatique ne se limite pas au hacking de gros systèmes informatiques appartenant à des banques ou à des administrations mais concerne aussi l'accès non autorisé à un terminal de télécommunication qui, en l'état actuel de l'art, est un ordinateur[117].

En d'autres termes, nous soutenons que le placement d'un numéro identifiant dans un terminal de télécommunication ou le simple accès à ce numéro ou à un autre identifiant du terminal constituent un accès majoritairement non autorisé. Il n'importe pas, dans ce cadre légal, de jauger la proportionnalité de tels procédés. L'autorisation demeure un acte positif qui

---

[115] Article 2 – Accès illégal : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

[116] Article 3 – Interception illégale : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

[117] Voir à ce sujet l'excellent article de Thierry LEONARD, « e-commerce et protection des données à caractère personnel : Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet » disponible sur http://www.droit.fundp.ac.be/Textes/Leonard1.pdf

se distingue de l'acceptation qui peut se déduire d'un silence éventuel ou de l'absence d'opposition.

Ainsi, on ne peut déduire, comme le fait DoubleClick[118], du simple fait qu'un utilisateur n'aie pas activé un inhibiteur de cookie, que l'utilisateur permet à tout quiconque de stocker ce type d'information sur son terminal.

5. Cinquième principe : L'octroi des moyens de protection des consommateurs, à l'utilisateur de certains systèmes d'information.

La banalisation de l'utilisation des technologies de l'information et de la communication, autrefois réservée aux seules entreprises et la généralisation de leur usage dans le développement du commerce électronique multipliant les services en ligne induisent une approche plus consumériste de la vie privée. C'est en tant que consommateur de ces services nouveaux que l'internaute ressent les atteintes à sa vie privée (spamming, profilage des internautes, politiques de différenciation des tarifs, refus d'accès à certains services, etc.).

Cette constatation explique qu' aux Etats-Unis, les premières velléités législatives en la matière de protection des données dans le secteur privé se soient appuyées sur la protection des consommateurs en ligne. Nous pouvons citer[119] à ce propos la loi californienne relative mais, au delà, on rappellera dès 1995 les premiers projets législatifs de « Consumer Privacy Act » et, plus récemment en 2000, la déclaration de la Federal Trade Commission[120] affirmant la nécessité d'une législation en matière de vie privée pour protéger les consommateurs en ligne. En Europe comme aux Etats-Unis, les dispositions prises pour lutter contre le spamming entendent protéger tant les intérêts économiques des consommateurs que la vie privée des personnes concernées.

Pistes de réflexion

- Cette convergence des intérêts de protection économique des consommateurs et des libertés des citoyens ouvre des perspectives intéressantes. Elle plaide pour reconnaître en matière de vie privée le droit à l'utilisation des moyens de recours collectifs, droit déjà reconnu en matière de protection des consommateurs. Ce droit à l'action collective, la « Class Action » américaine, est particulièrement important dans une matière où les

---

[118] Suite à une « class action » qui lui fut intentée il y a quelques années aux Etats-Unis, la pratique de DoubleClick consiste aujourd'hui à envoyer à tout terminal non identifié un premier cookie non rémanent et non identifiant qui se prénomme « accept cookies ». Si ce cookie est renvoyé, DoubleClick présume que le terminal accepte les cookies et envoie alors un cookie identifiant et rémanent pour une dizaine d'années (trente précédemment). Si le cookie n'est pas renvoyé, Double Click enverra indéfiniment ce cookie de demande d'autorisation. Un opt-out est prévu qui permet à l'utilisateur averti de stocker un cookie qui signifie qu'il n'en accepte pas.

[119] Cf. la California Online Privacy Protection Act (OPPA) en application depuis le 1er juillet 2004 qui insère des sections nouvelles (22575-22579) dans le « Business and professions Code » californien.

[120] Cf. le rapport au Congrès *« Privacy Online Fair Information Practices »,* Mai 2000, disponible sur le site de la FTC : http://www.ftc.gov/os/2000/05/index.htm . On note le rôle essentiel que joue aux Etats-Unis, la FTC, Commission active en matière de protection des consommateurs, dans la protection de la vie privée des citoyens américains

dommages subis par les personnes concernées sont souvent difficilement évaluables et où leur faible montant dissuade ces dernières d'un recours individuel

- Au-delà, toute une série de prescriptions du droit de la consommation trouveraient à s'appliquer utilement : on pense aux obligations d'information et de conseil qui pourraient être imposées aux opérateurs qui offrent des services impliquant essentiellement la gestion ou la délivrance de données personnelles (par ex : les fournisseurs d'accès à Internet ou les serveurs de bases de données nominatives (base de données jurisprudentielles, moteurs de recherche) , au droit des conditions générales contractuelles (applicables en matière de « privacy policy », à la lutte contre les pratiques déloyales en matière commerciale.

- Enfin, la cession volontaire de données nominatives, condition de l'accès à un site ou de l'obtention d'un service on-line pourrait s'analyser non seulement sur le plan de la loi de protection des données : le consentement donné par l'internaute répond t'il aux conditions de la définition du consentement et suffit-il à assurer la légitimité du traitement mais également sur le plan du droit de la consommation, ne serait-ce qu'en ce qui concerne la pratique déloyale quant à l'obtention du consentement ou la lésion grave que représente le déséquilibre de valeurs des données remises, d'une part, et du service obtenu, d'autre part.

- Une autre piste est la question de l'extension de la responsabilité du fait des produits de consommation (terminaux et logiciels) non seulement aux dommages physiques ou financiers mais aux atteintes à la protection des données. Dans quelle mesure, un fournisseur de logiciels de navigation dont le fonctionnement courant est générateur d'atteintes à la protection des données, ne pourrait-il se voir imputer une responsabilité objective du fait des atteintes à la protection des données réalisées par des tiers ?

CONCLUSIONS

Le contexte de l'Internet appelle une troisième génération de réglementations en matière de protection des données. Il ne s'agit pas de tourner le dos aux deux premières générations mais d'ajouter à celles-ci tout en ne modifiant pas les options déjà prises un niveau supplémentaire de protection. La première génération était essentiellement caractérisée par une approche fondée sur la nature de la donnée : était-elle sensible ? Appartenait-elle à la sphère intime de la personne concernée ? L'autodétermination informationnelle est alors comprise comme l'interdiction de traiter certaines données. C'est l'époque de la consécration de l'article 8 de la Convention européenne des droits de l'Homme. La deuxième génération ajoute à la première la nécessité, au delà de la protection de ces données particulières, d'envisager la façon dont le traitement de données à caractère personnel peut modifier les relations de pouvoir entre celui qui traite les données et celui à propos duquel le traitement a lieu. L'autodétermination informationnelle s'entend alors de la nécessité de rééquilibrer la relation en garantissant la transparence des traitements et en limitant le droit de traiter les données d'autrui. La Convention n° 108 est née dans cet esprit. Elle a fait de nombreuses émules et démontré ainsi amplement son bien fondé.

Ce qui caractérise la troisième génération que nous voyons poindre et dont nous souhaitons la consécration rapide est la prise en compte du fait technologique en lui même. Que l'utilisation de la technologie multiplie les données et les personnes capables d'y accéder, qu'elle accroît la puissance de ceux qui, grâce à elle, peuvent les collecter et mieux les traiter, qu'elle abolisse les frontières est un premier constat. La complexité du fait technologique, son opacité constituent une seconde réalité à prendre en compte. Entre la personne concernée et les maîtres du fichier s'invite une troisième personnage tour à tour « terminal » et « réseau ». L'autodétermination informationnelle passe dorénavant par une maîtrise de ce troisième personnage.

Pistes de réflexion :

Comment envisager cette maîtrise ? Nous présentons ci-après quelques pistes de réflexion sans prétendre épuiser le sujet :

- **"The answer to the machine is in the machine »: cette affirmation lancée par C. Clarke[121] à propos des problèmes rencontrés par la protection des droits d'auteur dans la société de l'information peut servir de guide pour trouver une réponse adéquate aux risques encourus par la vie privée du fait de la société de l'information. Ainsi, nous avons vu que le principe de réciprocité des avantages, la promotion de solutions technologiques « Privacy Minded » peuvent favoriser une meilleure maîtrise par la personne concernée de la circulation et de l'utilisation de son image informationnelle.**

- **A cet optimisme, nous avons mis des limites : si les technologies peuvent renforcer ce que certains appellent l'« User Empowerment », c'est au risque de laisser seule la personne concernée face au(x) maîtres du fichier. Ceci avec la circonstance que la technologie n'est pas neutre : si elle demeure largement « offerte » aux citoyens, elle est financée de manière indirecte par les entreprises et les administrations qui paient les ordinateurs serveurs. De manière**

---

[121] C. CLARKE, « Te answer to the machine is in the machine », in *The future of Copyright in a digital Environment,* B. HUGENHOLTZ (ed.), Kluwer, 1996, p. 139 et ss.

inéluctable, elle penche donc tout naturellement du côté des intérêts des ficheurs plutôt que vers la défense des fichés. La technologie dite de protection de la vie privée transforme ou risque de transformer la relation de l'individu à la donnée qui le concerne en une relation de propriété que la technologie permet de négocier. C'est le lieu de rappeler que l'autodétermination informationnelle est une liberté qui ne peut totalement se négocier et que c'est le devoir de la société de fixer certaines limites au droit de disposer de ces données.

- **Cette focalisation sur les outils technologiques doit amener à la prise en considération de nouveaux acteurs, non aperçus par les législations de deuxième génération : ainsi les fournisseurs de services de communication et les fournisseurs d'équipements terminaux. Leur rôle est décisif si on souhaite que l'utilisateur des services nouveaux de la société de l'information puisse contrôler les flux entrants et sortants de même que les traces laissées au fil des réseaux et leur possible utilisation. La responsabilité objective dans la fourniture d'équipements ou de services « privacy compliant » doit être envisagée.**

  Ainsi, en premier lieu, les fournisseurs d'accès à Internet, les opérateurs de mobilophonie ou de téléphonie se voient confiés la charge de sensibiliser le public sur les risques encourus lors de l'utilisation de leurs réseaux, de dénoncer les technologies « privacides » et, en même temps, de fournir un accès à des technologies « privaphiles » appropriées. Le rôle de ces fournisseurs d'accès est essentiel dans la mesure où ceux-ci représentent le point de passage obligé entre l'internaute et le réseau. Ainsi, leur demandera t'on[122] d'« informer l'internaute des moyens techniques qu'il peut utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications », d'utiliser les procédures appropriées et les technologies disponibles, de préférence celles faisant l'objet d'une certification, garantissant la vie privée et notamment l'intégrité et la confidentialité des données ainsi que la sécurité physique et logique du réseau… », « d'informer ces derniers (les internautes) des moyens d'utiliser ses services et de les payer anonymement ». Il offrira à ses abonnés une hotline leur permettant de dénoncer des violations de la vie privée et souscrira à un code de conduite suivant lequel il bloquera l'accès aux sites qui ne respectent pas les exigences posées en matière de protection des données et ce, peu importe la localisation du site.

  En second lieu, on vise les constructeurs et développeurs des matériels et logiciels qui conçoivent et construisent les équipements terminaux, ainsi que les responsables de l'élaboration des protocoles et des standards techniques utilisés pour transmettre des informations en réseau. Ils veilleront à concevoir des produits ou normes[123] :

  - **conformes, au cadre légal, par exemple par la transmission par les navigateurs internet des informations minimales nécessaires à la connexion ou par l'adoption de mesures de sécurité adéquates ;**

---

[122] Recommandation n° R (99)5, point III ; 1, 2 et 4

[123] Cf à ce propos, l'avis de la Commission belge n° 34/2000 à propos de la protection des données dans le cadre du commerce électronique.

- **qui facilitent l'application des principes dégagés ci dessus au titre II et qui permettent par exemple un accès direct par l'utilisateur à ses données personnelles ou un droit d'opposition automatique, notamment par le biais de journaux de bord ;**
- **et qui améliorent le niveau de protection des données à caractère personnel.**

- **L'outil technologique permet de plus en plus de traiter les données relatives à la personne concernée non point, comme c'était le cas de manière classique, par ses données d'identité légale (nom prénom, résidence, etc.) mais par un point d'ancrage voire par un objet (l'intelligence dite ambiante) qui lui est associé. Au delà, le danger n'est souvent plus dans la collecte a priori de données sur l'individu mais sur l'application a posteriori à un individu d'un profil abstrait…**
- **Le terminal, conçu au sens large, doit être traité comme un outil technologique totalement transparent pour celui qui en est le détenteur et l'utilise. Mieux, dans de nombreux cas, il appartient à la personne concernée et pourrait être assimilé à son domicile, c'est à dire au lieu où la personne se sent chez elle. L'intrusion dans ce domicile privé doit être traitée comme tout autre intrusion.**
- **L'opacité et la complexité des systèmes complexes d'informations auxquels les personnes concernées confient leurs données obligent à un surcroît d'informations non plus centrées sur le ou les traitements eux-mêmes pris séparément et sur leurs caractéristiques mais sur le fonctionnement global du système d'informations en tant que capable de générer une multitude de traitements présents ou à venir : ainsi, l'obligation de documenter les données (origine, utilisateurs, logique de raisonnement, d'établir un descriptif des circuits d'information) et de fixer les règles par lesquelles les décisions sont prises, les règles d'accès définies et contrôlées, etc .**
- **La prise en considération de l'outil technologique a jusqu' à présent peu été le fait de ceux qui ont à garantir la protection des données : les autorités de protection des données disposent rarement d'un informaticien, pénètrent rarement les cénacles de ceux qui décident des évolutions technologiques et de la configuration des produits. Sans doute faudrait-il comme les Etats européens ont exigé la création d'un Governmental Advisory Committee (GAC) auprès de l'ICANN, autorité privée qui décide de la gouvernance de l'Internet en matière d'adresses et de noms de domaines, suggérer voire imposer la création d'un Data Protection Advisory Committee auprès de l'ICANN, du W3C et de l'IETF ? La sensibilisation du milieu sectoriel de la communication électronique aux enjeux de protection des données s'avère nécessaire.**

En conclusion, les diverses pistes proposées à la discussion du Comité consultatif ont pour fils rouges

- de mettre à la disposition de l'individu tout ce qui est nécessaire pour comprendre et maîtriser son environnement informationnel en particulier celui qui pénètre son foyer. Il lui donne la maîtrise des outils dont l'utilisation le révèle à autrui ;
- de confier à la société les outils lui permettant de pouvoir continuer à maîtriser un développement technologique, dont l'enjeu est bien la survie de nos libertés tant individuelles que collectives.

Sur le réseau routier, la législation a imposé certaine règles à ses usagers afin, non seulement d'éviter des accidents, mais bien aussi de régler de manière équitable les droits et obligations réciproques des différents usagers de la route, avec en général, une propension prétorienne à protéger tout naturellement l'usager le plus faible. Pour ce faire, au-delà du code de la route, est apparue la nécessité d'une intervention législative toute particulière afin de réglementer le réseau routier lui-même ainsi que les véhicules qui sont admis à y circuler, moyennant le respect de certaines normes obligatoires.

Sur les autoroutes de l'information, il n'existe aucune législation qui s'attache à définir des normes de fonctionnement des télécommunications respectueuses de la protection de la vie privée des internautes ou encore des exigences de fonctionnement loyal et transparent des terminaux de télécommunication permettant aux internautes de circuler sur ces autoroutes.

Ce n'est pourtant qu'en appliquant les principes classiques de la protection des données à la technologie, ce troisième larron qui s'invite de manière implicite mais certaine dans toute télécommunication, que l'informatisation de la société pourra conduire à une société de l'information démocratique, moteur de progrès partout et pour tous.

Yves Poullet
yves.poullet@fundp.ac.be

Jean-Marc Dinant
jean-marc.dinant@fundp.ac.be

http://www.crid.be