Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection

Poullet, Yves

Published in:
Revue Lamy Droit de l'Immatériel

Publication date:
2005

Document Version
le PDF de l'éditeur

Le présent rapport établi pour la Conférence organisée à Prague les 14 et 15 octobre 2004 a pour objectif de répondre à la question suivante : « Comment, dans un monde globalisé, sensibiliser les personnes concernées par les dossiers sur leurs droits et responsabilités et en faire des acteurs de leur propre protection ? » (1). À bien la lire, la question évoque divers thèmes que nous soulignons d'emblée.

« Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection »

Par Yves POULLET
Doyen de la Faculté de Droit
FUNDP (Namur/Belgique)

Directeur du Centre
de Recherches Informatiques
et Droit (CRID)

1. La « *globalisation* » du monde préoccupe les défenseurs de la vie privée. Le monde est grâce aux réseaux devenu sans frontières. Mon curriculum vitae posté sur internet est accessible depuis les quatre coins de la planète. Les traces conscientes voire inconscientes que génère l'utilisation de mon ordinateur circulent *via* les réseaux et peuvent être collectées, traitées en de multiples endroits lointains ou non, connus ou inconnus de la personne concernée.
La globalisation génère des risques nouveaux : comment faire confiance à ces sites lointains parfois à peine identifiables et soumis à des réglementations parfois lacunaires sinon absentes ?
Le concept peut servir à désigner également l'omniprésence et la polyvalence croissante des réseaux et services de communication.
Les réseaux se multiplient tout en étant interopérables(GPS/RFID/GSM/Wifi/BlueTooth/GRPS/SMS, etc.), leur capacité et leur interactivité croissent. De plus en plus d'objets sont dotés d'une puce qui les connecte aux réseaux et, se multiplient les usages humains ayant recours à ces réseaux. Lire un journal, payer son fournisseur, placer une petite annonce, ouvrir son garage, chercher un emploi, une information, une rue, discuter avec des copains, commander un livre ou réserver un voyage, choisir un film, ... quelle occupation peut encore échapper aux possibilités croissantes offertes par les technologies de l'information et de la communication ! Nous voilà saisis par les TIC (Technologies de l'information et de la communication) dans notre globalité.

2. La question suggère deux types d'action vis-à-vis des personnes concernées : « *sensibiliser* » et « *rendre acteurs* ».
À l'amélioration de la situation passive de la personne concernée, mieux informée, mieux éduquée, et plus attentive dès lors au respect de ses droits, s'ajoute la volonté des auteurs de la question de rechercher les moyens par lesquels la personne concernée peut, elle-même, veiller et accroître sa protection.
Chacune de ces actions se trouve facilement justifiée.
Pourquoi une sensibilisation plus grande est-elle nécessaire ? Sans doute, parce que les capacités croissantes des ordinateurs et les réseaux multiplient les traitements et leurs qualités. Sans doute, parce que c'est de plus en plus la personne concernée qui, de par son utilisation des réseaux, génère des données de plus en plus nombreuses et riches. Sans doute, surtout parce que de plus en plus de traitements qui nous entourent sont mal identifiés voire opaques.
On ajoutera à ces arguments le sentiment ressenti par de nombreux utilisateurs de la perte de maîtrise de l'équipement terminal, c'est-à-dire d'un objet en leur possession qui permet la connexion et l'utilisation du réseau. La notion d'équipement terminal est large : il s'agit de tout produit ou composant d'un produit (2) qui rend possible la communication et qui est connecté directement ou indirectement et ce par tout moyen à des réseaux de télécommunications publics. Si spontanément on évoque téléphone, mobilophone ou équipements PC, il faut également songer aux cartes, lecteurs de cartes, aux *Radio Frequency Identifiers* (RFID), et à tous les systèmes de télémétrie qui permettent de repérer à distance la personne ou un objet relatif à une personne identifiable. À l'égard de ces terminaux, J.M. Dinant (3) parle de « *changement de paradigme social* » : « *L'appareil possède toujours un déterminisme qui n'est plus dicté par l'utilisateur mais bien plus 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 observable* (par exemple : décrocher le téléphone et avoir une tonalité, recevoir un appel et déclencher la sonnerie) *mais constitue l'appel à un programme informatique qui possède l'autonomie de faire ce que l'utilisateur de-*

(1) Le rapport n'engage que son auteur. Il est le fruit de réflexions personnelles et ne prétend en rien représenter les vues des commanditaires du rapport ni des instances auxquelles l'auteur du rapport appartient.

(2) *Cf.* à cet égard la directive n° 99/5/CE sur l'équipement terminal de radio ou de télécommunications.

(3) Dinant J.M., Projet de rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Doc. Provisoire, Strasbourg, 20e réunion, 28-30 juin 2004.

mande, si le programmeur l'a décidé. Qui plus est, ce comportement est généralement en partie inobservable à l'œil nu » (4).

À la boîte noire que représente le terminal, s'ajoute celle que représentent les vastes systèmes d'information et de communication de nos grosses entreprises et de nos administrations. L'information ne se définit plus au sein de ces systèmes par une ou deux finalités statique(s) mais par leurs possibilités de réutilisation à l'infini au sein de ces systèmes évolutifs et ce, afin de satisfaire des besoins au départ non identifiés ou ne pouvant être satisfaits. La donnée personnelle, de plus en plus, est envisagée au sein de ces vastes systèmes d'information comme une donnée déposée, susceptible d'être reprise par les multiples utilisateurs du système pour des finalités non définies à l'avance. Ainsi, même la donnée relative à une prescription médicale peut se trouver sur une carte de santé et demain être susceptible tantôt d'être reprise à des fins de contrôle des prescripteurs, tantôt à des fins statistiques de santé publique, tantôt à des fins de remboursement, tantôt à des fins d'intervention en cas d'urgence, etc.

3. Pourquoi, dans un second temps, insister sur le rôle actif de la personne concernée et la rendre responsable de sa propre protection ?

L'interactivité des réseaux, en même temps, nous l'avons dit, qu'elle multiplie les données générées par la personne concernée, autorise cette dernière à mieux négocier la protection de ses données : limiter le type d'utilisation de celles-ci et de leurs utilisateurs.

Par ailleurs, on connaît la mode des « *Privacy Enhancing Technologies* (5) », qui, sous des formes diverses, créent le sentiment d'un « *User Empowerment* » (6), prétendant rétablir un certain équilibre entre les collecteurs de données et les personnes concernées.

Enfin, la personne concernée apparaît, tant vis-à-vis des actions de sensibilisation que de celles qui seraient mues par les personnes concernées, comme sujet à la fois de droits et d'obligations. La personne concernée a le droit à la protection des données mais, dans le même temps, serait responsable d'adopter un comportement limitant les risques d'atteinte à la protection de ses données.

Une telle conception mettant à charge de la personne concernée le devoir de contribuer à sa propre protection se retrouve déjà en filigrane de la « *Recommandation du Conseil de l'Europe à propos de la protection des données sur l'internet* » (7).

Elle heurte la réalité d'une personne concernée placée dans une situation proche du consommateur, c'est-à-dire dans une situation de faiblesse tant économique que technologique. Dans ce contexte, la réglementation vise à protéger le faible, la personne concernée contre le fort, le responsable du traitement et dès lors adresse à celui-ci un certain nombre d'obligations et de responsabilités. Certes, on pourrait demain concevoir que certaines obligations légales soient également adressées à la personne concernée, afin de limiter ses propres risques mais cela suppose que

L'interactivité des réseaux, en même temps qu'elle multiplie les données générées par la personne concernée, autorise cette dernière à mieux négocier la protection de ses données : limiter le type d'utilisation de celles-ci et de leurs utilisateurs.

soient respectées de manière efficace des règles de protection mises à charge des maîtres de fichier. Pour prendre un exemple dans un autre domaine, n'est-ce pas après avoir contraint les fabricants de voitures à installer des ceintures de sécurité que le port de la ceinture a été imposé aux conducteurs ? Nous reviendrons sur cette comparaison (8).

4. La question à l'origine du rapport, telle que posée, laisse bien percer tant l'angoisse que l'espoir de l'interrogateur. Elle suggère en effet qu'aux risques nouveaux d'atteinte à la vie privée, ceux nés de la globalisation, de l'opacité et des capacités croissantes des réseaux, l'internaute puisse grâce à l'interactivité des réseaux et à des solutions technologiques mieux se protéger, voire mieux assumer ses responsabilités.

5. Répondre à la question nous obligera dans un premier temps à décrire les apports respectifs que chaque mode de réglementation peut apporter à la résolution de la question soulevée. À cet égard, on examinera dans un premier temps (I) les mérites relatifs des régulations publiques, celles de l'autorégulation et finalement de la technologie avant de conclure à la nécessité d'une corégulation.

Nous poursuivrons sur la nécessité, vu le contexte nouveau, de définir de nouveaux principes qui devraient orienter des régulations nouvelles (II). Pour faire bref, il apparaît que la sensibilisation des personnes concernées et la prise de responsabilités par ces dernières prennent vis-à-vis des systèmes d'information modernes une nouvelle dimension et exigent des contenus de régulation nouveaux quelles que soient leurs sources.

Enfin, on s'attardera (III) aux solutions que chaque acteur de la société de l'information peut apporter dans la mise en place de ces solutions. Traditionnellement, les législations « *privacy* » se limitent à envisager trois acteurs : principalement les responsables de traitement et les personnes concernées, d'une part et, d'autre part, chargés d'éclairer l'un et l'autre et d'aider à la définition de l'équilibre des intérêts de ces deux protagonistes, les autorités de protection des données, celles publiques visées par nos législations de protection des données (9).

Les réglementations récentes laissent apparaître de nouveaux acteurs dont le rôle est peut-être plus décisif encore : les associations de consommateurs, les fournisseurs de services de télécommunications, en particulier les fournisseurs d'accès au réseau et surtout les fabricants d'équipements terminaux.

---

(4) À cet égard, l'exemple des « *cookies* » qui a révélé ce malaise de l'utilisateur qui apprend que son ordinateur bavarde ou babille sans contrôle de l'internaute.

(5) L'expression fut utilisée pour la première fois en août 1995 par le rapport commun de l'« *Information and Privacy Commission* » de l'Ontario et de la « *Registratiekamer* » des Pays-Bas, The path to Anonymity, Achtergrond syudies en Verkenningen 11, Den Haag, 2 volumes, 2e éd., 1998.

(6) Sur cette notion utilisée également à propos des « *PICS* » dans un autre débat à savoir celui en matière de liberté d'expression, lire MM. d'Udekem-Gevers-Poullet, Internet Content Regulation – Concerns from an European User Enmpowerment Perspective, 17 CL&SR 2001, p. 371 et s., 18 CL&SR 2002, p. 11 et s.

(7) Cf. de manière cependant très nuancée, la Recommandation n° R(99)5 du Comité des ministres aux États membres sur la protection de la vie privée sur internet, adoptée par le Conseil des ministres le 23 février 1999 : « *L'utilisation d'internet implique une responsabilité pour chaque action et comporte des risques pour la vie privée. Il est recommandé de se conduire de manière à se protéger et à promouvoir de bonnes relations avec les autres* ».

(8) ... que nous devons à notre collègue du CRID des FUNDP, Jean Marc Dinant.

(9) On notera que l'intérêt de ce troisième acteur n'a été que très récemment reconnu par le Conseil de l'Europe soit en 2001 lors de la signature du Protocole additionnel à la Convention pour la protection des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, Strasbourg, 8 novembre 2001. Ce protocole « *vise à renforcer la protection effective de l'individu en rendant nécessaire la création d'une ou plusieurs autorités de contrôle qui contribuent à la protection des droits et libertés de l'individu à l'égard du traitement des données à caractère personnel* ».

I. – TROIS MODES DE RÉGULATION AU SERVICE DE LA SENSIBILISATION ET DE LA RESPONSABILISATION DES UTILISATEURS DE SERVICES D'INFORMATION ET DE COMMUNICATION : LA LOI, L'AUTORÉGULATION ET LA TECHNOLOGIE – PLAIDOYER POUR LA CORÉGULATION

6. Le propos de ce titre n'est pas d'analyser de manière détaillée le contenu de chacun des modes de régulation traditionnellement invoqué pour assurer la protection des données : la loi, l'autorégulation et la technologie (10). Seule nous importe la manière dont ces trois modes, séparément, dans un premier temps, de manière combinée ensuite, peuvent contribuer à une meilleure information de la personne concernée quant à ses droits et à un meilleur exercice de ceux-ci.

A. – La loi

7. Nos législations de protection des données ont, à la suite de l'article 8 de la Convention n° 108, accordé des droits à la personne concernée. Ces droits assurent à cette dernière une certaine maîtrise de leur image informationnelle. On cite ainsi le droit d'être informé de l'existence des traitements, le droit d'accès, le droit de correction et de recours.

Il est intéressant de noter que nos législations modernes ont élargi ces droits à la mesure des défis rencontrés vu la complexité croissante des systèmes d'information. En particulier, l'accès aux données depuis la directive européenne n° 95/46/CE (11) ne se conçoit plus comme le seul accès au contenu des données, mais également à leur origine et surtout à la logique du traitement. La même directive n° 95/46 a créé le droit de ne pas être soumis à une décision prise sur la base d'un traitement automatisé de données, ce qui oblige au dialogue avec la personne concernée. Plus récemment la directive n° 2002/58/CE (12) a exigé le consentement pour l'envoi « *à des fins de prospection directe* » de communications électroniques.

Cette extension ne s'arrête pas à la reconnaissance de droits nouveaux pour la personne concernée mais affirme des obligations nouvelles à charge des responsables de traitement. À cet égard, on cite le récent *California Online Privacy Protection Act* (OPPA) qui impose à tout prestataire de services web qui collecte des données (13) de créer une page web comprenant certaines informations (14).

8. Si des droits nouveaux sont ainsi législativement consacrés, on s'aperçoit que leur exercice reste limité voire inexistant. Les deux Eurobaromètres (15) publiés en 2003 par la Commission européenne en témoignent : 49 % des entreprises déclarent avoir reçu moins de 10 demandes d'accès en 2002 et 25 %, aucune. On connaît la suite : « *Pour la plupart des entreprises, constatent les auteurs de l'Eurobaromètre relatif à la perception par les entreprises des législations de protection des données, la conformité à la loi n'est pas une priorité puisqu'elles reçoivent peu de plaintes* ».

Sans doute, ceci est-il dû à la faible connaissance par les personnes concernées tant de la question de la protection des données et de ses enjeux (70 % des Européens estiment que la protection des données est méconnue) que de l'existence des lois instituant cette protection (seuls 32 % (16) ont entendu parler du droit d'accès, de rectification ou de suppression). Une autre raison est à notre avis la relative confiance des citoyens dans les mesures prises par leur pays même s'ils ignorent le contenu de ces mesures. On souligne l'effet pervers d'une intervention réglementaire qui déresponsabilise ceux qui devraient être les premiers acteurs de leur protection : les personnes concernées.

9. On ajoute que la lecture des lois de protection des données décourage le lecteur non initié voire l'avocat par son caractère abstrait et trop général. Comment le citoyen peut-il traduire des dispositions aussi absconses que celle suivant laquelle le responsable du fichier ne peut traiter des données de manière incompatible avec les finalités de la collecte lorsqu'il se trouve destinataire d'un e-mail envoyé par sa banque lui annonçant que sa prime d'assurance accident doit être augmentée vu les risques supplémentaires liées à la perte de son emploi, à ses mauvais placements boursiers ou simplement l'intérêt de contracter auprès d'elle une assurance moins chère que celle prise auprès d'un concurrent dont l'existence lui est révélée par un virement effectué ? Ce fait est relevé par nombre de citoyens : n'est-ce point un comble de constater cette difficulté de lecture pour une loi censée apporter au citoyen protection et maîtrise de son environnement ?

Ainsi, la loi n'est pas par sa seule vertu garantie d'effectivité.

B. – L'autorégulation

10. L'autorégulation, présentée comme le modèle alternatif à la régulation publique, peut être tentante. Les « *Privacy Policies* », simples « *commitments* », « *Codes of Practices* » ou « *Privacy Standards* » (17) émanant des responsables de traitement, seuls ou encadrés, comme c'est le cas dans les « *Safe Harbor Principles* » (18), fleurissent. Ils présentent l'avantage pour la personne concernée de développer, dans un langage bien plus convivial que celui de la loi, des principes plus adaptés à la réalité des traitements d'une entreprise ou d'un secteur.

Les reproches adressés à l'autorégulation sont connus : le premier est le manque de garantie quant à l'effectivité de ce mode de régulation. À cet égard, il faut distinguer suivant les différents types d'autorégulation signalés plus haut. Le Privacy « *commitment* » est un engagement de l'entreprise. Le Privacy « *Code of Practice* » est défini à un niveau plus collectif, ainsi par un secteur professionnel. Les membres de ce « *collectif* » >

---

(10) Sur ces trois modes, lire en particulier, Reidenberg J., Privacy Protection and the Interdependence 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 s. ; Bennett C.J. et Raab C.D., The gouvernance of Privacy, Ashgate, 2003, p. 12 et s.

(11) Directive n° 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, JOCE 23 nov. 1995, n° L 281, p. 31 et s.

(12) Directive n° 2002/58/CE du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE 31 juill. 2001, n° L 201, p. 37 et s.

(13) Ce texte voté en 2003 est en application depuis le 1er juillet 2004. Il insère des sections nouvelles (22575-22579) dans le « *Business and Professions Code* » californien.

(14) En particulier, on note outre les informations exigées traditionnellement par nos législations (l'identité du maître du fichier, le type de données collectées, les finalités d'utilisations), des données plus spécifiques au caractère éphémère des contenus des sites web, ainsi les procédures de modification et la date de la « *Privacy Policy* ».

(15) *Cf.* les deux Eurobaromètres publiés par la DG Marché intérieur et disponibles sur le site : <www.europa.eu.int/commun/international_market/privacy>. Le premier (Eurobaromètre Spécial 196, septembre 2003 s'attache plus à l'opinion des citoyens européens, le second (Eurobaromètre Flash 147, septembre 2003), à celle des entreprises.

(16) Parmi cette catégorie, seuls 7 % avaient utilisé le droit d'accès.

(17) Sur la différence entre ces trois types d'autorégulation, Bennett C.J. et Raab C.D., The gouvernance of Privacy, Ashgate, 2003, p. 12 et s.

(18) *Cf.* à cet égard, la décision n° 2000/520/CE de la Commission conformément à la directive n° 95/46/CE du Parlement européen et du Conseil relative à la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes, publiées par le ministère du Commerce des États-Unis d'Amérique, JOCE 25 août 2000, n° L 215, p. 7 et s. L'encadrement par les pouvoirs publics est assuré par le fait que les « *Safe Harbor Principles* » ont été négociés avec les pouvoirs publics et que les déclarations de conformité sont publiés sur le site officiel du Department of Commerce. Sur ces « *Safe Harbor Principles* » comme mode de corégulation, lire Poullet Y., Les Safe Harbor Principles ; Une protection adéquate, disponible sur : <www.droit-technologie.org>.

adhèrent aux principes et des sanctions, en cas de non-respect, peuvent être prévues par l'association qui a établi le code. Enfin, les « *Standards* » impliquent une procédure d'évaluation du respect de leur contenu par ceux qui déclarent les respecter. Cette procédure peut consister en une « *certification* » (19) de la conformité des traitements aux principes déclarés et la délivrance d'un label (20) La définition de normes (21), dont le respect fait l'objet de vérifications et d'audit, est une autre procédure évoquée.

Le recours en cas de non-respect peut se voir facilité par la mise sur pied d'« *Alternative Dispute Resolution Mechanisms* » (ADR) (22) auxquels l'accès est facile, dont la compétence est évidente et par lesquels des solutions plus adaptées et constructives peuvent être trouvées.

Ainsi, le reproche du manque d'effectivité, s'il apparaît évident vis-à-vis des formes « *faibles* » d'autorégulation, est à nuancer fortement vis-à-vis de ses formes plus avancées. Cependant, on déplorera la multiplication des labels et la difficulté d'en saisir la portée et parfois le contenu. L'autorégulation sauvage met à charge de la personne concernée le soin de vérifier la qualité de celle-ci (23).

11. Un deuxième reproche souligne les dangers du caractère « *volontaire* » de l'autorégulation. Sans doute, dira-t-on, l'absence de tout engagement ou la prise d'engagements à contenu faible amèneront les personnes concernées à préférer l'entreprise concurrente qui s'est soumise à une autorégulation plus contraignante et à contenu plus protecteur. Une telle affirmation résiste peu à l'analyse lorsqu'on sait que parfois le choix n'existe point et qu'en toute hypothèse, le critère « *Privacy Protection* » n'est pas le plus déterminant dans le choix des personnes concernées.

Un troisième reproche porte sur le contenu de la protection offerte. Les « *standards* » définis sont souvent faibles dans la mesure où leur définition relève souvent des seuls responsables de traitement, préoccupés de ne point trop augmenter leurs charges.

C. – Les solutions technologiques

12. Les solutions technologiques (24) dites « *Privacy Enhancing Technologies* » (PETs) sont invoquées, avec de plus en plus d'insistance, soit comme outil de protection des données à l'appui de solutions autoréglementaires comme le P3P (25), soit comme substitut aux autres modes de régulation comme la cryptographie (26).

À noter que ces solutions réglementaires peuvent être implémentées au niveau de l'infrastructure, ainsi on pourrait imaginer le blocage automatique des connexions vers des pays ne respectant pas les prescrits en matière de protection des données, au niveau du responsable du traitement, au niveau d'intermédiaires comme l'utilisation de filtres par des serveurs spécialisés chargés de bloquer les « *spams* » adressés par certains types d'entreprise ou, enfin, au niveau des terminaux de la personne concernée comme les outils de blocage de l'envoi et de réception de « *cookies* » ou de négociation avec le responsable du traitement.

13. Les critiques de tels outils, dont on souligne l'effectivité (27), tiennent au contenu des règles qu'elles mettent en œuvre. Ces règles sont souvent négociées au sein de cercles d'experts, peu au courant des exigences de la protection des données ou plus sensibles aux besoins du monde professionnel qu'aux intérêts de la personne concernée. On dénonce également à propos des technologies dont la mise en œuvre dépend des personnes concernées elles-mêmes, le mythe de l'« *User Empowerment* ». Dans quelle mesure la personne concernée peut-elle prendre en charge sa protection au moment où la transparence des conséquences de ces décisions n'est pas assurée et où les choix n'existent pas toujours ? Ainsi, combien de sites ne refusent-ils pas l'accès aux utilisateurs qui n'acceptent pas les « *cookies* » ? La négociation *via* le P3P risque elle-même d'être faussée lorsque le responsable du traitement propose insidieusement de « *payer* » l'obtention des données personnelles. Bref, comme l'écrit Dix (28) : « *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* ».

D. – La nécessaire convergence des trois modes de régulation

14. 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 sensibiliser (29). 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. Les réalités et conformité de la pratique aux prescrits légaux peuvent être laissées à l'appréciation de certificateurs ou d'auditeurs (30) dont l'intervention sera démontrée 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. À défaut, peut-être faut-il prévoir une intervention législative (31) qui fixera ces divers points.

(19) Ainsi, celle de Trust-e, du BBB Online, Privacy Programme, de Webtrust, etc.

(20) Sur ces techniques de « *labellisation* », Reidenberg J.R., Adapting Labels and Filters for Data Protection, Cybernews, 1997, III, p. 6.

(21) On rappelle l'exemple canadien du « *Model Code for the Protection of Personal Information* », approuvé par le « *Standards Council of Canada* » en mars 1996. Plus récemment, les discussions menées au sein de l'ISO.

(22) À noter que les « *Safe Harbor Privacy Principles* » font de la désignation d'un ADR un élément essentiel de la mise en œuvre (Enforcement) du système mis en place : « *Pour protéger efficacement la vie privée, il convient de mettre au point des mécanismes permettant d'assurer le respect des principes de la sphère de sécurité, de ménager un droit de recours aux personnes concernées par le non respect des principes et de sanctionner les organisations... Ces mécanismes doivent comprendre au minimum : a) des systèmes de recours indépendants aisément accessibles et peu coûteux, permettant d'étudier et de résoudre toute plainte et tout litige...* ».

(23) Sur ce point, Solové D. J., Privacy and Power : Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review (2001), 1393 et s.

(24) Burkert H., Privacy Enhancing Technologies Typology, Critique, Vision, in Agre P. and Rotenberg M. (eds), Technology and Privacy, MIT Press, Cambridge, M.A., p. 125-143 ; Lessig L., Code and other Laws of Cyberespace, Basic Books, New York, 1999, p. 26 et s ; Reidenberg J., Lex Informatica : the Formulation of Information Policy through Technology, 76 Texas Law Rev., 1998, p. 552-593, Poullet Y., Technology and Law : from Challenge to Alliance, Information Quality Regulation : Foundations, Perspectives and Applications, U. Gasser (ed.), Nomos Verlagsgesellschaft, 2004, Pour une présentation des PETs, voir le site de l'EPIC : <www/epic.org/privacy/tools.html>.

(25) A propos du P3P, lire J. Catlett, Technical Standards and Privacy : An open letter to P3P developers, article disponible sur le site : <www.junkblusters.com/standards.html>.

(26) Sur les différents protocoles d'encryptage et les serveurs d'anonymisation de même que sur les instruments d'anonymisation ou d'utilisation de pseudonymes, lire C.J. Bennett et C. D. Raab, op. cit., p. 148 et ss.

(27) À cet égard, les conclusions du projet PISA sur lequel nous reviendrons (infra) : « *Privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing ... rather than relying on legal protection and self-regulation.* » (<www.dbs.cordis.lu/fep>).

(28) A. Dix, Infomediaries and Negociated Privacy Techniques, papier présenté à la Conférence « *Computers, Freedom and Privacy* » (CPF 2000), 19 avril, Toronto, disponible à : www.portal.acm.org/citation).

(29) Sur ce point, lire Reidenberg J.R., Privacy Protection and the Interdependence 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 s.

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* ».

15. Un autre exemple est certes la régulation des labels de certification des sites web en matière de « *Privacy* » (32). La multiplication des labels induit la confusion de l'internaute. Quelle valeur accorder à 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 (33).
Bref, les solutions sont à trouver, on le pressent, dans un « *effective mix* », un système de corégulation (34) où la loi trouve non seulement son prolongement mais également son effectivité dans des systèmes techniques et d'autoréglementation qu'elle doit appeler de ses vœux et promouvoir.

II. – QUELQUES NOUVEAUX PRINCIPES POUR FAVORISER LA SENSIBILISATION ET LA RESPONSABILISATION DES PERSONNES CONCERNÉES

16. Les caractéristiques mêmes de l'environnement des services de communications électroniques : omniprésence et polyvalence croissante des réseaux de communications électroniques et des terminaux, interactivité de ceux-ci, dimension internationale des réseaux et services et producteurs d'équipement, opacité de fonctionnement des terminaux et réseaux, multiplient 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 leur donnant une meilleure maîtrise de leur 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.
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. – Le principe de l'encryptage et de l'anonymat « réversible »

17. L'encryptage des messages assure la protection de l'accès au contenu des communications. Leur qualité varie et les techniques d'encryptage et de décryptage peuvent également être diverses. Les logiciels d'encryptage placés sur l'ordinateur de l'internaute (protocoles S/MIME ou Open PGP) sont désormais accessibles à des prix abordables. La notion d'anonymat quant à elle devrait sans doute être définie et peut-être d'autres concepts comme « *pseudonyme* » ou « *non-identifiabilité* » devraient être préférés dans la mesure où cette notion est 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 (35). Nombre de textes à caractère non contraignant préconisent le « *droit* » du citoyen (36) 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 (37) énonce : « *L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée* ».

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 sensibiliser.

18. Celui qui utilise les moyens modernes de communication doit 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 (38). La mise à disposition à des coûts abordables de moyens ou de services d'encryptage et d'anonymisation est une condition nécessaire à une responsabilisation de l'internaute.
L'anonymat ou la « *non-identifiabilité* » requis ne sont cependant pas absolus. Au droit à l'anonymat des citoyens s'oppose l'intérêt supérieur de l'État qui pourra imposer des limitations lorsque celles-ci constituent des mesures nécessaires « *pour sauvegarder la sûreté de l'État, 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 organisées par celle-ci, pourrait s'opérer le lien entre l'identité réelle d'un usage et son pseudonyme. Au-delà, d'autres solutions pourraient être imposées par une réglementation des appareils terminaux : suppression >

(30) 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.
(31) Ainsi, huit 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-Billy Act* ».
(32) Sur la régulation des labels de certification, lire les recommandations de l'E-confidence Forum disponible sur le site . <www.jrc.it>.
(33) *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.
(34) Sur la corégulation, lire Poullet Y., Technologies de l'information et de la communication et « co-régulation », une nouvelle approche ?, in Mélanges Coipel, Kluwer, à paraître.
(35) Sur ce point, lire Gnijpink J. et Priens C., Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions ?, 17 CL&SR § (2001), p. 378 et s.
(36) À ce propos, lire notamment Rodota S., Beyond te E.U. Directive : Directions for the Future, in Privacy : New Risks and opportunities, Poullet Y., de Terwangne C. et Turner P., Cahier du CRID, Kluwer, Antwerpen, n° 13, p. 211 et s.
(37) « *Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "nforoutes"* », 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 nov. 2000, disponible sur le site de la Commission belge de la vie privée : <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.
(38) *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 (Georges M., 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).

du « *bavardage* » des navigateurs, la création d'adresses éphémères 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.

B. – Le principe de réciprocité des avantages

19. 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 mesure « *proportionnée* » des avantages de la technologie.

Quelques dispositions récentes se fondent sur l'exigence de proportionnalité 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.

Citons ainsi la directive européenne n° 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 n° 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 doit faire l'objet d'une information de ce dernier et que celui-ci dispose du droit de refuser un tel traitement ...* ».

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. Récemment, une commission suédoise (39) 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 plus facilement un document spécifique. Une proposition de loi proposerait même que les documents officiels qui sont à la base d'une décision puissent d'une manière ou d'une autre être liés aux autres documents relatifs au cas. À 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.

20. 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.

En matière de protection des données, on peut 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 :

– 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 média 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. Enfin, pourquoi ne pas imaginer que l'accès à un site situé dans un pays ne bénéficiant pas d'une protection adéquate soit automatiquement signalé ;

– le droit d'accès de la personne concernée doit demain pouvoir s'exercer *via* le média électronique sur la base de l'utilisation d'une 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 (40) 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 « *déposée* » 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* » (41) ;

– 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 ;

– le droit de recours, également, ne mériterait-il pas de pouvoir bénéficier des avantages que représente la cyberma-

(39) Seipel P., Information System Quality as a Legal Concern, in Information Quality Regulation : Foundations, Perspectives and Applications, Gasser U. (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.

(40) *Supra*, note 3.

(41) 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 (L. 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 (L. 16 janv. 2003 portant création d'une Banque Carrefour des entreprises, M. B. 5 févr. 2003, article 19 § 4).

gistrature, 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 ?

C. – Le principe de promotion de solutions technologiques conformes ou améliorant la situation des personnes protégées par le droit

21. La Recommandation 1/99 du 23 février 1999 (42), émise par le Groupe dit de l'article 29 sur la 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.

22. Ainsi, il s'agit pour eux de pouvoir intervenir en cas de développements technologiques présentant des risques majeurs. Ce principe dit de précaution largement connu en droit de l'environnement pourrait trouver à s'appliquer en matière de protection des données.
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 manière – 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* » (43). 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 aptes 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 (44), 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.

23. 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'État, 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 nécessaires à la protection des données.

D. – Le principe de la maîtrise par l'utilisateur du fonctionnement des équipements terminaux

24. 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 n° 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.
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, auprès de tiers fiables (45), être certaine de la désactivation de ce moyen technique de repérage à distance.

25. On note que ce principe, l'usager l'opposera 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. Nous reviendrons sur ce point lors de notre analyse des acteurs (III).
Au-delà, il s'adresse aux organes de normalisation tant publics que privés qui s'occupent 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 de ceux-ci va bien au-delà de ce qui est strictement nécessaire à l'établissement de la communication ;

(42) Recommandation sur les traitements invisibles et automatiques de données à caractère personnel sur Internet réalisés par des logiciels et matériels.
(43) Selon l'expression de Dinant J. M., Law and technology Convergence in the Data Protection Field, in E-commerce Law and Practice in Europe, Walden I. et Hörnle J., Woodhead Publishers Ld, Cambridge, 2002, Chapter 8.2.

(44) Sur le design « *privacy compliant* » de ces cartes multiapplications, lire les réflexions de Keuleers E. et Dinant J. M., Multi-application smart card schemes, 19. CL&SR, 4 2003, 480 et s ; 20, CL&SR, 1, 2004, 22 et s.

(45) On songe bien évidemment à des systèmes de labellisation comme ceux décrits, *supra* n° 14 (corégulation) ou à des agréments donnés par l'autorité publique à certaines entreprises (régulation publique).

- 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 navigateurs des traitements, des traitements déloyaux seront plus ou moins faciles ;
- l'utilisation d'« *Unique identifiers* » ou de logiciels espions par les fournisseurs d'outils de navigation ou de logiciels de communication est également à signaler.

Au-delà de ce premier souci, on met en évidence l'idée 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 fichiers reçus, leur finalité et leur émetteur.

E. – Le principe de l'octroi des moyens de protection des consommateurs à l'utilisateur de certains systèmes d'information

26. La banalisation de l'utilisation des technologies de l'information et de la communication, autrefois réservées 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 États-Unis, les premières velléités législatives en matière de protection des données dans le secteur privé se soient appuyées sur la protection des consommateurs en ligne. Nous avons déjà cité (46) à la loi californienne 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* (47) affirmant la nécessité d'une législation en matière de vie privée pour protéger les consommateurs en ligne. En Europe comme aux États-Unis, les dispositions prises pour lutter contre le « *spamming* » entendent protéger tant les intérêts économiques des consommateurs que la vie privée des personnes concernées.

27. 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 la « *Class Action* » est particulièrement important dans une matière où les 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 exemple : 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 « *online* » pourrait s'analyser non seulement sur le plan de la loi de protection des données : le consentement donné par l'internaute répond-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 ?

III. – LE RÔLE DES ACTEURS TRADITIONNELS ET NOUVEAUX DANS LA SENSIBILISATION ET LA RESPONSABILISATION DES PERSONNES CONCERNÉES

28. Bien des choses ont été dites à propos des obligations mises à charge des responsables de traitement. Ces obligations prennent, grâce aux technologies de l'information et à cause de ces technologies, une dimension nouvelle. La Recommandation n° R(99)5 du Comité des ministres aux États membres sur la protection de la vie privée sur internet (48), résume en son point III.11 les points essentiels : « *Vous êtes responsables de la bonne utilisation des données. Sur votre page de bienvenue affirmez par une indication claire et visible votre politique en matière de vie privée. Cette indication devrait permettre par un hyperlien d'accéder à une explication détaillée de vos pratiques en la matière. Avant que l'utilisateur ne commence à utiliser des services, lorsqu'il visite votre site et chaque fois qu'il en fait la demande, informez-le de votre identité, des données que vous collectez, traitez et conservez, de quelle manière et pour quelles finalités. Au besoin demandez-lui son consentement. À la demande de la personne, rectifiez sans attendre les données inexactes, effacez-les si elles sont excessives, si elles ne sont pas mises à jour, et arrêtez le traitement si la personne concernée s'y oppose* (...). *Notifiez aux tiers auxquels vous avez communiqué les données toute modification. Évitez toute collecte à l'insu de l'intéressé* ».

29. Nous nous arrêterons plus longuement sur les devoirs d'un deuxième acteur traditionnel : les autorités de protection des données dont le rôle est essentiel dans l'économie de nos législations de protection des données même si le Conseil de l'Europe n'a reconnu ce rôle que tardivement (49). Il s'agit à travers ces autorités notamment de fournir une assistance et une aide aux personnes concernées et de promouvoir l'« *awareness* » des règles de protection des données tant auprès des responsables que de ces personnes (50).

(46) *Supra* note 12.

(47) *Cf.* le rapport au Congrès « *Privacy Online Fair Information Practices* », Mai 2000, disponible sur le site de la FTC : <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.

(48) Adoptée le 23 février 1999.

(49) *Cf.* le protocole additionnel à la Convention n° 108 concernant les autorités de contrôle et les flux transfrontières de données (STE, n° 181, Strasbourg, 8 nov. 2001).

(50) Ces rôles ont été mis en évidence au niveau européen par le Groupe dit de l'article 29 en particulier lors de l'analyse de la notion de protection adéquate (*cf.* en particulier, le Working Paper n° 12 adopté le 24 juillet 1998 : « *Transferts de données à caractère personnel vers des pays tiers : application des articles 25 et 26 de la directive communautaire sur la protection des données* »).

Chez nous, ce rôle est assuré par les autorités administratives indépendantes. L'Eurobaromètre déjà cité atteste du peu de répercussions de l'activité de ces autorités souvent frileuses – administration oblige –, plus soucieuses de procédure et de juridisme que d'être un réel acteur de terrain. On se souvient à cet égard des critiques adressées en son temps par Flaherty lors d'une Conférence internationale des Commissaires à la Protection des données : plus des deux tiers des Européens (68 %) déclarent ne pas connaître l'existence de ces autorités et seuls 27 % déclarent en avoir entendu parler (51).

Ce constat est alarmant. L'absence de ces autorités dans les médias, même à l'occasion d'événements portés sur la scène publique, est certes à souligner. Mais une visite des sites de ces autorités atteste d'autres défauts. Peu de sites sont attractifs (52). Peu de sites permettent le dépôt de plainte en ligne (53). L'ouverture sur certains thèmes de forums de discussion n'est présente que sur quelques sites. Seuls quelques-uns ont fait l'effort d'une présentation sous forme de FAQ des lois de protection des données (54). On regrettera l'absence de liens vers des sites, qu'ils soient universitaires, professionnels ou autres (associations de consommateurs, « *civil liberties* ») permettant d'en savoir plus (55). On déplorera que ces sites n'offrent pas de description de produits et services technologiques permettant une protection effective (56).

Le manque de ressources budgétaires est sans doute une explication mais est-elle suffisante ?

Bref, des autorités trop fermées sur elles-mêmes devraient trouver des relais d'information et d'actions communes auprès d'autres groupes de protection des citoyens.

(51) Seuls les Pays-Bas, l'Italie et la Suède comptent plus d'un habitant sur trois ayant entendu parler de cette autorité. Dans ce contexte, la solution québecoise consistant à mettre à la tête de la Commission d'accès à l'information et à la protection des données un journaliste n'est pas à dédaigner.

(52) On excepte le site de la CNIL.

(53) *Cf.*, à ce propos, les divers modèles d'introduction de plainte proposés par la Federal Trade Commission.

(54) *Cf.* le site néerlandais en particulier : <www.cbpweb.nl/documenten/faq_wbp_cbp.htm> et celui anglais : <www.informationcommission.gov.uk> qui propose également des vidéo et CD Rom particulièrement bien construits mais malheureusement non disponibles en ligne. Le site de la CNIL propose en outre une démonstration en ligne de la façon dont l'internaute est reconnu lors de la visite d'un site web.

(55) Sans doute faut-il y voir à nouveau un indice de la frilosité de nos autorités soucieuses de ne pas apparaître comme privilégiant certaines opinions ou certaines institutions ?

(56) ... ce que EPIC (Electronic Privacy Information Centre) propose avec des hyperliens (*cf.* <www.epic.org>).

30. La sensibilisation des personnes concernées et des responsables de traitement ne peut en effet être le seul fait des autorités de protection des données. Au-delà du rôle que pourraient jouer à cet égard les associations dites de libertés civiles et de protection des consommateurs si la notion de recours collectif était acceptée (57), on pointe d'autres acteurs. Le premier est désigné par l'article 4 de la directive n° 2002/58 : « *Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque* (58) *et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en indiquant le coût probable* ».

Ainsi, les fournisseurs d'accès à internet, les opérateurs de mobilophonie ou de téléphonie se voient confiés la charge

Des obligations mises à charge des responsables de traitement prennent, grâce aux technologies de l'information et à cause de ces technologies, une dimension nouvelle.

de sensibiliser le public sur les risques encourus lors de l'utilisation de leurs réseaux, de dénoncer les « *Privacy Killing Technologies* » et, en même temps, de promouvoir les « *Privacy Enhancing Technologies* » appropriées. Le rôle de ces fournisseurs d'accès est essentiel dans la mesure où il représente l'interface obligé entre l'internaute et le réseau. Ainsi, leur demandera-t-on (59) 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* ». Ils offriront à leurs abonnés une « *hotline* » leur permettant de dénoncer des violations de la vie privée et souscriront à un code de conduite suivant lequel ils bloqueront 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.

(57) *Supra* note 27

(58) *Cf.* déjà le point III.2 de la recommandation n° R(99)5 du Conseil de l' Europe citée à de nombreuses reprises.

(59) Recommandation n° R(99)5, point III ; 1, 2 et 4.

31. Deux autres types d'acteurs ont déjà été mentionnés. Il s'agit, premièrement, de tous les tiers de confiance dont l'activité relève en principe des lois de marché. Ces acteurs offrent des services. Certains permettent aux personnes concernées d'être rassurées quant au respect des prescrits de protection des données, il s'agit alors de services d'accréditation et de certification qui, par les « *infomédiaires* », se présentent comme des interfaces entre la personne concernée et les responsables du traitement offrant des services d'anonymisation, des services de filtrage ou de négociation avec les responsables. Sans doute, ces nouveaux médias devraient être mieux connus et leurs activités promues par les pouvoirs publics (60)

En second lieu, on vise les constructeurs et développeurs des matériels et logiciels qui constituent 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 ce que la configuration de leurs produits ou normes (61) :

- soit conforme 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 ;
- facilite l'application des principes dégagés ci-dessus au titre II et qui permette par exemple un accès direct par l'utilisateur à ses données personnelles ou un droit d'opposition automatique ;
- et qui améliore le niveau de protection des données à caractère personnel. >

(60) Ainsi, *via* des contrats de recherche permettant la mise au point de nouveaux services ou produits. L'exemple de PISA (Privacy Incorporated Software Agent), projet subsidié par le Ve programme cadre de l'UE, mérite d'être signalé. Sur ce programme et la comparaison entre l'approche « *PISA* » et celle du P3P (la première visant à rétablir une situation d'égalité entre la personne concernée et le site web), voir le site : <www.tno.nl/instit/fel/pisa> et les réflexions de Borking et Raab, Laws, PETS and other Technologies for Privacy Protection, JILT, 2001, p. 1 et s (disponible également sur le site : <elj.werwick.ac.uk/filt/01-1/borking .html>).

(61) *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.

32. Venons-en précisément aux rôles de ces derniers. L'État, selon la jurisprudence du Conseil de l'Europe, a l'obligation de promouvoir les libertés de ces citoyens. À ce titre, il ne peut considérer que son rôle se limite à celui de contrôler et de sanctionner les éventuels abus. Risquons sur ce point quelques suggestions.

La conscientisation des personnes concernées ne peut être le seul fait des autorités de protection des données. Les principes mêmes de la protection des données doivent être enseignés en même temps que l'école ouvre ses élèves à l'utilisation des technologies de l'information et de la communication.

La conscientisation des responsables de traitement peut se faire par la création de modules de formation universitaire ou non destinés aux « *détachés à la protection des données* » (62) ou plus largement aux responsables « *sécurité* » (63) des administrations et entreprises. Il s'agit ainsi d'instiller le souci du respect des principes de protection des données au cœur des entreprises et administrations.

Vis-à-vis des autres modes de régulation, le devoir de promotion des nouveaux services et produits et de veiller à une corégulation à laquelle participent tous les acteurs concernés par la protection des données a déjà été rappelé. On ajoutera, vis-à-vis des développements technologiques, un « *devoir de précaution* ».

L'introduction de technologies nouvelles en particulier celles liées à l'utilisation des réseaux de communication doit être l'objet d'une analyse des impacts de ces technologies sur les libertés fondamentales. Ce « *Technology Assessment* » (64) doit conduire à des débats publics dont l'organisation peut être confiée aux autorités de protection des données et peut aboutir à des décisions suspendant le développement de ces technologies au résultat d'expérimentation. Il va de soi que ce rôle, l'État ne peut le jouer que s'il est présent dans les organisations généralement purement privées où se décident les futurs développements technologiques (65).

Enfin, l'État doit, à propos des traitements dont il est lui-même le responsable, veiller au-delà du simple respect des prescrits, à promouvoir des solutions qui renforcent les droits de la personne concernée. À l'heure de l'« *e-government* » et des guichets uniques, comment ne pas se servir des applications réseaux mises en place pour permettre au citoyen l'accès électronique à son dossier, le suivi de l'origine des données y inscrites et des personnes ayant reçu communication de ses données et une information complète en langage convivial des systèmes de communication interadministration qui permettent la gestion des dossiers relatifs aux citoyens ? Des sites web explicatifs des différentes finalités des traitements administratifs et du mode de fonctionnement du système d'information qui permet d'accomplir ces finalités et la mise en place de « *hot lines* » permettant la réception de plainte et de plateformes de médiation au sein de l'administration pourraient constituer des modèles susceptibles d'être repris par le secteur privé.

L'introduction de technologies nouvelles en particulier celles liées à l'utilisation des réseaux de communication doit être l'objet d'une analyse des impacts de ces technologies sur les libertés fondamentales.

CONCLUSION

L'introduction soulignait la part d'angoisse que recelait le titre même du rapport qui m'était demandé. L'appel à une meilleure sensibilisation et aux responsabilités des personnes concernées laissait entendre qu'à l'heure de la double globalisation (66) que représentent les technologies de l'information et de la communication, la maîtrise par ces personnes dites concernées sur l'utilisation de leur image informationnelle avait singulièrement diminué. En cause, la boîte noire que représentent des terminaux de plus en plus complexes et « *intelligents* » et des systèmes d'information sans frontières, aux capacités de traitement illimitées.

Pour redonner à l'utilisateur, tant soit peu, une certaine maîtrise, la loi apparaît d'un faible secours. À la faible connaissance par les citoyens des droits que généreusement la loi leur accorde répond en écho la faible propension des maîtres de fichier à respecter une loi peu invoquée. Cette constatation ne condamne pas en soi la loi mais invite à chercher dans des solutions autoréglementaires voire technologiques des relais à des meilleures traductions et une effectivité renforcée des droits de la personne concernée. La solution est à trouver dans la corégulation, c'est-à-dire le dialogue fécond entre ces différentes techniques de régulation.

Nous le répétons : la loi est nécessaire... Elle oriente les initiatives autoréglementaires 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 réaliseraient certaines technologies de négociation reste un mythe s'il n'est soumis au contrôle de la loi.

L'appel à la corégulation suppose la promotion de nouveaux acteurs, qui aident à la sensibilisation et offrent à l'utilisateur des possibilités réelles de maîtrise de son environnement, ainsi les certificateurs de sites web, les infomédiaires. Elle conduit à 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.

Ce dernier point et cet exemple constitueraient deux des principes nouveaux dont nous réclamions la reconnaissance. On rappellera les autres : la maîtrise par la personne concernée de la circulation de son image informationnelle dans les systèmes modernes d'information passe à la fois par une totale transparence du fonctionnement des terminaux en sa possession, tout comme par un surcroît d'informations non plus centrées sur le traitement lui-même et ses caractéristiques mais sur le fonctionnement du système

(62) À cet égard, les propositions faites par la délégation belge à la conférence des commissaires à la protection des données réunis à Buenos Aires.

(63) On n'insistera jamais assez sur le fait que la protection des données a un but plus large que la seule « sécurité » des traitements. Il s'agit au-delà de la protection de la confidentialité des données de veiller à un équilibre entre les intérêts du responsable du traitement et ceux des personnes concernées par le traitement.

(64) À cet égard, Flaherty D., Privacy Impact Assessments : An essential Tool for Data Protection, 7 PLPR (2000), p. 85 et s.

(65) On vise bien évidemment l'IETF, le W3C, l'ICANN. Sur ces organisations, lire Trudel P., Droit du cyberespace, Montréal, Thémis, 1997 ; Berleur J., Poullet Y., Quelles régulations pour l'Internet, Gouvernance de la société de l'information, Cahier du CRID, n° 22, Bruylant, Bruxelles, p. 133 et s.

(66) Globalisation dans un premier sens, de par la dimension internationale des réseaux et de leur convergence ; globalisation dans un second sens, dans la mesure où l'ensemble de nos activités, qui progressivement se voit traduit en information digitale.

d'informations en tant que capable de générer une multitude de traitements : ainsi, l'obligation de documenter les données (origine, utilisateurs, logique de raisonnement), d'établir un descriptif des circuits d'information.

Ces divers principes ont pour but essentiel de mettre à la disposition de l'individu tout ce qui est nécessaire pour comprendre son environnement informationnel, en particulier celui qui pénètre son foyer. Il lui donne la maîtrise des outils dont l'utilisation le révèle à autrui.

Sans doute, l'acquisition de cette maîtrise suppose que divers acteurs l'accompagnent. À cet égard, nous avons plaidé pour que les autorités de protection des données soient plus attentives à l'écoute du citoyen et lui offrent une information plus conviviale, nous avons souligné le rôle d'éducation que l'État peut jouer tant vis-à-vis des maîtres de fichier que des personnes concernées, celui également de promotion tant des outils que des métiers nouveaux. Nous pensons que les fournisseurs d'accès doivent, comme interface obligé entre le réseau et la personne concernée, être les relais de l'information sur les risques du réseau et sur les moyens de les parer. Enfin, la responsabilité des producteurs d'équipements terminaux est évidente.

Ainsi, les inforoutes se trouvent sécurisées : les infrastructures de communication et les nœuds « *routiers* » bien balisés, les voitures qui y circulent munies des équipements de sécurité nécessaires et les conducteurs dûment sensibilisés aux risques de la conduite et disposant d'équipements fiables pour éviter les dangers...

Il reste alors à ces derniers de prendre leurs responsabilités et de devenir acteurs de leur propre protection. ◆