État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement

Pierre TRUDEL*

Sommaire

Dans l'univers des réseaux, l'information est persistante et circulante. Tenter d'en empêcher la circulation au cas où elle pourrait être mal utilisée est une approche de moins en moins efficace.

Le ciblage défectueux du droit de la protection des données personnelles — hérité des approches prévalant dans les années 70-80 affaiblit la protection de la vie privée des personnes. Ces approches nient la légitimité de la circulation de certaines informations dans les espaces publics sans pour autant assurer une protection effective des informations vraiment relatives à la vie privée. Le risque de voir se développer un ensemble de règles incompatibles avec les exigences de l'État de droit paraît suffisamment important pour justifier des interrogations sur le cadre juridique actuel et les approches qui pourraient en augmenter l'efficacité.

Devant les rigidités découlant de ces interprétations abusives, tant les administrations que les législateurs ont été amenés à recourir à des expédients comme le développement de pratiques de gestion du consentement et on a multiplié les lois d'exception, affaiblissant la protection des données personnelles. Pire, on a négligé de rendre plus efficaces les règles à l'encontre des pratiques vraiment attentatoires à la vie privée en accordant peu d'attention à l'application effective des lois sur la protection des données dans les situations où les risques de dérives sont importants.

* Titulaire de la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, Faculté de droit, Université de Montréal. Courriel : pierre.trudel@umontreal.ca.

La modernisation effective du droit de la protection des données personnelles passe par une relecture critique des fondements de la législation et des applications qui en a été faite. Une telle relecture exige une évaluation lucide des contextes dans lesquels circulent désormais les informations. Ce serait affaiblir le droit à la vie privée que de se réfugier dans une frileuse défense des mécanismes formalistes hérités des époques antérieures. Une telle approche accroît les risques d'une protection de plus en plus factice.

Table des matières

Introduction....3

I- La protection des données personnelles selon le schéma classique....5
A) Des fondements devenus inadéquats....6
1. Le droit à la vie privée....6
2. Des extrapolations apocalyptiques....8
3. Des périls mal ciblés....10
4. Une fuite en avant : de la vie privée à la « vie personnelle »....13
B) Une application de plus en plus laborieuse....15
1. L'illégitimité des espaces publics....15
2. La rigidification du principe de finalité....19
3. Le recours machinal au consentement comme palliatif à la rigidité....22
4. La multiplication des lois d'exceptions....24

II- Pistes pour renforcer la protection de la vie privée dans les réseaux....25
A) Une lecture actualisée des principes de protection des données personnelles....26
B) L'impératif de confiance....30
C) Le droit à une technologie compatible avec la protection de la vie privée....31
D) La maîtrise des données personnelles....32
E) L'exigence de qualité....34
F) Des mécanismes effectifs de sanction....35

Conclusion....37

INTRODUCTION

Le contexte de la circulation des informations portant sur les personnes connaît des changements significatifs. Les systèmes d'information se conçoivent désormais comme des réseaux, c'est-à-dire des environnements interconnectés dans lesquels l'information circule d'un pôle à l'autre, de façon multidirectionnelle et non hiérarchique. De tels environnements redéfinissent les espaces dans lesquels circulent les informations relatives aux personnes. Ce phénomène est manifeste dans le secteur public où se profilent de plus en plus des projets de mise en place de services publics en ligne voire de « gouvernement électronique ».

La généralisation des activités susceptibles de se dérouler désormais de plus en plus dans des environnements comme Internet requiert une meilleure prise en compte de l'espace dans lequel circulent les données personnelles avec la place accrue que prend désormais le virtuel[1]. Il devient en effet nécessaire de revoir les notions qui aident à déterminer ce qui doit être protégé comme relevant de la vie privée et l'information qui doit circuler puisqu'elle participe à l'espace public, contribue au déroulement de la vie sociale ou à assurer le bon fonctionnement des services publics.

Le cadre juridique actuel postule le caractère exceptionnel des transferts de données personnelles sans le consentement des personnes visées. En dépit de ce caractère exceptionnel, force est de constater que les transferts de renseignements personnels sont considérables entre certains organismes publics. Dans la plupart des pays, le partage de renseignements est autorisé mais généralement de façon à augmenter la duplication de données d'un organisme vers l'autre. Cette approche encourage la duplication et, compte tenu de la persistance de l'information, accroît la quantité de renseignements personnels détenus par les Administrations.

Un double phénomène de personnalisation et de mise en commun de l'information caractérise plusieurs tendances accompagnant

---

[1] Vincent GAUTRAIS, « Le défi de la protection de la vie privée face aux besoins e circulation de l'information personnelle, » *Lex electronica*, vol 9 no. 2, hiver 2004, < http://www.lex-electronica.org/articles/v9-2/gautrais2.htm>.

l'émergence de l'administration électronique. La circulation et le partage des informations permettent d'améliorer la qualité et la célérité des prestations. En réduisant la redondance, en limitant les situations dans lesquelles les personnes sont obligées de retransmettre les mêmes informations, on réalise des gains de productivité qui devraient globalement profiter à tous.

Il est de plus en plus prévisible que les citoyens s'attendront à interagir avec l'État comme ils sont en voie de s'habituer à le faire avec les autres prestataires de biens et de services en ligne. Le citoyen s'attendra à ce que les informations pertinentes aux rapports qu'il entretient avec l'État soient disponibles au moment où elles sont nécessaires et que ces informations possèdent les qualités appropriées pour les fins auxquelles elles doivent servir. Par exemple, le citoyen qui change d'adresse pourra transmettre l'information pertinente en un seul lieu et lors d'une seule opération afin qu'elle soit relayée à tous les organismes devant être informés du changement.

Dans la première partie, l'on propose une revue critique plusieurs concepts fondateurs du droit de la protection des données personnelles. On démontre que ceux-ci doivent être adaptés aux exigences découlant de la généralisation des réseaux. On relève le caractère trop simplificateur de la notion de données personnelles, les effets pervers du paradigme de la « surveillance » qui est sous-jacent à l'interprétation dominante du droit actuel de la protection des données personnelles. Ce paradigme mené à des interprétations englobantes de ce que recouvre la notion de données personnelles. Il a favorisé une interprétation rigide de plusieurs notions de même qu'une tendance à complexifier ou interdire la circulation des informations qui n'ont pourtant que peu à voir avec la vie privée. Des expédients ont dû être surdéveloppés afin de pallier à ces dérives au plan de l'interprétation des lois sur la protection des données personnelles. Le résultat de cette évolution est une complexité inutile et coûteuse au plan de la protection de la vie privée.

Dans la seconde partie, sont présentés les éléments d'un cadre actualisé capable d'assurer effectivement la protection des données personnelles dans les espaces de réseaux consacrés aux services publics.

I- La protection des données personnelles selon le schéma classique

Le droit relatif à la protection des données personnelles existe depuis près de trois décennies. Principalement issu d'un mouvement véhiculant les appréhensions à l'égard des périls de l'informatique centralisée, il s'est construit en forme de rempart contre les risques de surveillance par les autorités étatiques. Ses fondements ont fait l'objet de peu de débats. Un auteur a même avancé qu'il s'agissait de « législation symbolique » caractérisée notamment par un faible ancrage sur la demande sociale[2]. La rituelle référence à quelques sondages faisant état du fait que les populations s'inquiètent à propos de leur vie privée tient habituellement lieu de justification aux interprétations rigides des règles relatives à la protection des données personnelles. Dans la plupart des pays, on a généralement pris pour acquis que les techniques utilisées par les législateurs et par les instances de régulation étaient généralement appropriées. Par contre, ces législations demeurent méconnues et l'on éprouve des difficultés à en assurer une application effective[3].

L'accroissement de la circulation de l'information modifie l'échelle des risques pour la protection des personnes. La généralisation des réseaux induit des mutations au niveau de la raison d'être des règles de droit. D'où les revendications constantes pour un renforcement de la protection de la vie privée des personnes lors de la mise en place des environnements de traitement de l'information. Mais il est de loin d'être certain que c'est en reconduisant les approches héritées des modèles existants de protection des données personnelles que l'on assurera un encadrement effectif de la production et de la circulation des données personnelles.

Afin de garantir l'effectivité du régime de protection de la vie privée dans le contexte des environnements ouverts, il faut revoir certaines

---

2 Pierre SADRAN, « De l'efficacité des politiques symboliques : l'accès à l'information et la transparence administrative, » dans Pierre TRUDEL (éd.) *Accès à l'information et protection des données personnelles*, Montréal, P.U.M., 1984, p.29.

3 Voir: Valérie SÉDALLIAN, La loi informatique et liberté: du mythe à la réalité, <europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/sedallian_en.pdf >.

des prémisses fondant le régime actuel de la protection des données personnelles. Dans un monde où cette information circule de plus en plus, ce n'est plus contre les risques de surveillance qu'il faut diriger le cadre juridique de la protection des données personnelles mais plutôt vers l'utilisation adéquate et balisée de l'information relative aux personnes. Ce n'est plus en mettant des entraves à la circulation de l'information qu'on assurera le respect de la vie privée mais en encadrant de façon appropriée et effective, la collecte, l'utilisation, la circulation et le maintien de la qualité de l'information portant sur les personnes.

A) Des fondements devenus inadéquats

Le droit de la protection des données personnelles a été conçu pour protéger la vie privée contre les écueils que laissait craindre l'utilisation des technologies de l'information à des fins de surveillance. À l'usage, il s'est avéré que le droit de la protection des données personnelles ne vise pas tant à contrer la surveillance que d'assurer la qualité de l'information dans le cadre des processus décisionnels. Mais la persistance du paradigme de la surveillance a conduit à étendre la portée et l'interprétation de certaines notions au point de transformer ce qui devait protéger la vie privée en une protection tous azimuts de la vie personnelle. Ce glissement des fondements du droit de la protection des données empêche un recentrage des efforts afin d'assurer l'effectivité de la protection de la vie privée.

1. Le droit à la vie privée

Le droit à la protection des données personnelles constitue une facette des régimes de protection de la vie privée. Il existe une étroite relation entre les règles relatives à la protection des données personnelles et la possibilité effective pour une personne de maîtriser la circulation de l'information la concernant. Mais la notion de données personnelles est née d'un souci de simplification. Pour contourner les difficultés de dégager ce qui doit rester dans le secret au nom du droit à la vie privée, on a opté pour une notion qui confond « renseignements qui identifient une personne » avec les « renseignements sur sa vie privée. » Ainsi, au nom de la protection de la vie privée, s'est mis en place un ensemble de règles

visant, non plus les informations portant sur la vie privée mais sur l'ensemble des informations susceptibles d'identifier les personnes.

Le droit à la vie privée varie en fonction du contexte, des époques, des moeurs et, surtout, de la position occupée par les personnes dans la société. Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information ou une intrusion porte sur un élément de la vie privée. Le domaine de la vie privée regroupe certains types d'informations qui y sont, en principe, rattachées. Le domaine de la vie privée connaît aussi des variations selon les qualités et la situation des personnes. On identifie traditionnellement deux grands volets à la vie privée. Le premier réfère aux faits et aux aspects de la vie d'une personne qui sont inclus dans un domaine protégé. Il permet d'identifier les éléments considérés comme inclus dans le domaine de la vie privée d'une personne, à une époque donnée. Mais le contenu concret de ce domaine varie suivant les personnes, la position qu'elles occupent dans la société et d'autres circonstances. C'est le volet qui prend en considération les personnes visées. Ce volet contextuel permet d'apprécier le contenu du domaine de la vie privée en fonction des circonstances, notamment la participation de l'individu à la vie de la collectivité[4]. Bien peu de ces ont été conservées avec le recours à l'englobante notion de « renseignements susceptibles d'identifier une personne » qui est au cœur de la plupart des lois sur la protection des données personnelles.

L'adoption d'une notion englobante de données personnelles procédait d'un souci de disposer d'une définition claire des informations portant sur les personnes et qui devaient êtres protégés. On cherchait à s'affranchir des difficultés découlant du caractère fluctuant et contextuel de la notion de vie privée. C'est manifestement à un souci de simplicité que répondait l'adoption de cette notion. Si l'on convenait que plusieurs données personnelles relatives à une personne relevaient de sa vie privée, il était aussi entendu que tous les renseignements sur une personne ne relèvent pas uniquement de sa vie privée. Malgré cela, on a fréquemment laissé de côté les nuances qui caractérisaient jusque-là le concept de vie privée.

---

4 Patrick A. MOLINARI et Pierre TRUDEL, « Le droit au respect de l'honneur, de la réputation et de la vie privée : Aspects généraux et applications », dans Barreau du Québec, Formation permanente, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, 197p. 211.

Le résultat de ce glissement a été d'assimiler toute donnée sur une personne à sa vie privée et de protéger cette dernière en censurant, sans distinction, tous les renseignements relatifs à une personne. Les craintes que s'instaurent des pratiques de « surveillance » ont accentué la distorsion introduite dans le droit à des fins de commodité. On en est venu à considérer que toute donnée concernant une personne identifiable pouvait avoir un rapport avec la vie privée de cette dernière. La légitimité associée à la protection de la vie privée et à la dignité humaine a été mobilisée afin de justifier des mécanismes qui ne respectent pas toujours les équilibres qui doivent exister entre les divers droits concernés par la circulation de l'information.

2. Des extrapolations apocalyptiques

Plusieurs affirmations au sujet des risques de la circulation de l'information pour les personnes se fondent sur des extrapolations alarmistes. Habituellement, l'on invoque le potentiel d'abus découlant de la puissance des technologies de l'information. On escompte que le potentiel d'abus sera nécessairement et universellement réalisé et réclame des mécanismes interdisant a priori les opérations qui sont perçues comme potentiellement risquées.

Cette approche n'est pourtant pas celle qui prévaut à l'égard de plusieurs autres types de risques technologiques et sociaux. Par exemple, on ne prohibe pas l'usage des automobiles sur les routes au motif que certains conducteurs utilisent ces outils de manière inadéquate ou carrément dangereuse.

À ce jour, les cas connus de surveillance découlant des traitements de données personnelles relèvent de l'anecdote. La plupart concernent les opérations de surveillance policières qui échappent à toutes fins pratiques à la portée des lois sur la protection des données personnelles. On retrouve quelques incidents ayant eu pour conséquence de laisser circuler des informations personnelles de façon inappropriée. Dans plusieurs cas, c'est la pénurie de ressources ou le manque de volonté pour appliquer les dispositions existantes des lois qui paraît expliquer les difficultés Mais à moins d'étendre le sens du mot surveillance, c'est en vain que l'on cherchera des pratiques généralisées de surveillance des personnes.

Devant les possibilités théoriques que procurent les technologies de l'information, on en vient à invoquer la crainte de la surveillance, non plus pour désigner les activités de surveillance qui se déroulent effectivement mais celles qui pourraient devenir possibles si des informations étaient traitées de façon malveillante. On entre alors dans un cycle d'auto-justification : ayant proclamé de grands dangers, l'on cite ensuite des sondages tendant à indiquer que les citoyens ont cru à ces pronostics alarmistes et s'inquiètent des dangers pour la vie privée susceptibles de découler de l'accroissement des traitements d'informations personnelles.

Malgré la rareté des tentatives d'en vérifier l'application réelle, le paradigme de la « surveillance » s'est traduit par une constante rigidification et bureaucratisation des mesures de protection des données personnelles. Pour éviter la surveillance, il fallait que l'information soit confinée à l'organisme qui l'a collecté, qu'elle ne circule que moyennant consentement éclairé de l'intéressé et ce peu importe le degré de sensibilité de l'information. Le dossier médical d'une personne est mis sur le même pied que son adresse de courriel! Pour prévenir la surveillance, il faut éviter que l'information ne circule. On va donc préférer la redondance à la réutilisation de l'information. Peu importe que le citoyen soit obligé de recommencer les mêmes démarches plusieurs fois ! Peu importe que l'on multiplie les banques de données contenant les mêmes données personnelles ! Pourvu que l'information soit confinée dans autant d'alcôves administratives et qu'elle ne serve qu'à une seule finalité !

Cette approche ignore les dynamiques de fonctionnement des réseaux et accroît la détention globale de données personnelles. Comme il est en principe interdit d'obtenir des données personnelles autrement qu'en les réclamant de la personne concernée, il faut recollecter et recollecter les mêmes données, accumuler et sur-accumuler des données personnelles dans toujours plus de banques de données de plus en plus difficiles à contrôler.

À une époque où se généralise l'usage des technologies de l'information, il faut des fondements plus solides et mieux ciblés. On ne peut se limiter à reconduire indéfiniment les frayeurs d'une époque où l'on assimilait tous les usages des technologies avec les abus dont elles peuvent faire l'objet. Des mesures aussi mal ciblées pourraient mener à l'affaiblissement des protections de la vie privée.

3. Des périls mal ciblés

Plusieurs interprétations des lois sur les informations personnelles sont essentiellement fondées sur des craintes et des extrapolations. Daniel J. Solove relève que les appréhensions à l'égard des banques de données personnelles ne sont pas adéquatement articulées[5]. Les médias, les décideurs politiques et les juristes décrivent les problèmes engendrés par le traitement de l'information relative aux personnes en se fondant sur la métaphore du Big Brother tirée du roman 1984 de George Orwell. Une littérature foisonnante justifie la nécessité des lois sur la protection des données personnelles en se fondant sur les possibilités que s'instaure une société de surveillance semblable à celle décrite par Orwell dans son célèbre roman[6].

La frayeur que la technologie inspire à plusieurs caractérise - et de façon nettement dominante- les analyses et les discours au sujet des menaces et des risques que les technologies représentent pour les personnes. Mais comme on se représente le traitement de l'information comme menant invariablement à la surveillance, on en déduit que la généralisation des outils capables de servir à de telles fins va nécessairement engendrer de plus grandes menaces. Lucas, Devèze et Frayssinet, écrivent à cet égard que :

> [...] les nouvelles technologies constituent un puissant outil bureaucratique et technocratique devenu essentiel pour la rationalisation de la gestion publique, l'action de la police et de la justice, la conduite des politiques publiques (santé, emploi, aides publiques…), la lutte contre les fraudes, la

---

5 Daniel J. SOLOVE, « Privacy and Power : Computer Databases and Metaphors for Information Privacy, » [2001] 53 *Stanford L. R.,* 1393, p. 1395.

6 Il est intéressant que l'on souligne si peu un autre aspect de la société décrite par Orwell dans *1984* : une société où des préposés du « ministère de la Vérité » passent leur temps à réécrire l'histoire, faisant disparaître le nom et les photos de ceux que le pouvoir à éliminé ! Cela ressemble à la tendance induite par ceux qui réclament que les données publiques, telles les banques de décisions judiciaires et sans doute celles des journaux soient purgées de leur nom. Ainsi, au nom d'une conception totalitaire de la protection de la vie personnelle, on en vient à censurer jusqu'aux archives historiques !

> prévision. Pratiquement toutes les actions administratives passent par un fichage.[7]

Ces analyses reflètent de ce que Daniel J. Solove appelle la « métaphore du Big Brother ». Mais, lorsqu'on y regarde de près, la protection des données personnelles ne répond pas à des dangers de surveillance. Elle vise plutôt à assurer que les informations sur les personnes soient de qualité.

Dans les argumentations justifiant les mesures de contrôle des données personnelles, on prend acte des possibilités offertes par la technique et on conclut aussitôt à l'éventualité d'usages abusifs. On invoque machinalement les supposés risques de surveillance ou les dramatiques « vols d'identité » ou pareilles fantasmagories illustrées par la littérature ou une certaine cinématographie. Par contre, lorsque vient le temps de documenter les dangers qui guettent effectivement les personnes du fait de la circulation des données personnelles, on évoque, non plus des problématiques de surveillance, mais plutôt des problématiques tenant à la qualité des informations lors des processus décisionnels. On fait alors le constat que :

> Le danger provient du caractère inadéquat, équivoque, imprécis, disproportionné de l'information collectée parfois de manière déloyale par rapport à une finalité critiquable qui peut s'abriter derrière un argumentaire la présentant de manière favorable.[8]

Dans cet esprit, on souligne le fait qu'il n'y a pas de « données anodines ». Lucas, Devèze et Frayssinet relèvent que :

> La pratique démontre qu'il n'y a pas de données anodines et que la notion de données sensibles (santé, opinion politique ou syndicale, vie privée) définie a priori doit être considérée de manière relative; après tout, les sociétés de vente par correspondance ne demandent pas l'âge de leurs

---

7 André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis Droit privée, 2001, p. 10.

8 André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis. n° 18.

> clientes car cela est mal perçu; mais grâce aux tables d'attribution des prénoms de l'INSEE, elles déduisent avec une forte probabilité l'âge des personnes.[9]

Suivant un tel raisonnement, même le prénom d'une personne serait une information pouvant relever de sa vie privée en ce que cela permettrait de connaître son âge par recoupement. Mais l'âge que l'on attribuerait à la personne dans une telle situation est celui que permettrait d'évaluer le processus de comparaison avec une donnée à caractère historique : les tables annuelles d'attribution des prénoms. Il serait ainsi possible de savoir qu'une Nathalie est possiblement née entre 1965 et 1972. On voit que ce qui pose ici problème n'est pas tant la menace à la vie privée car on ne divulgue pas l'âge effectif de la personne. On a plutôt ici une donnée à caractère probabiliste fondée sur le fait qu'une personne née entre telle et telle année a beaucoup de chances de porter tel ou tel prénom. Il serait évidemment absurde d'utiliser de telles informations afin de prendre une décision significative à l'égard d'une personne. On constate que nous ne sommes pas ici en présence d'une atteinte à la vie privée. C'est plutôt un problème de qualité d'information. Si cette information sur l'âge des personnes obtenue via ce genre de recoupement est possiblement suffisante pour mener des opérations de ciblage en marketing, elle est nettement insuffisante pour prendre la moindre décision à propos d'un individu.

L'exemple est extrême mais il illustre l'intérêt de fonder la protection des données personnelles non sur les risques de surveillance, mais en donnant plus d'importance aux garanties de qualité de l'information. L'exemple illustre aussi les écueils de confondre toutes les informations relatives à une personne et la vie privée de cette dernière. Enfin, il met en lumière le fait que les problèmes auxquels vient répondre le droit de la protection des données personnelles sont souvent des problèmes de qualité de l'information utilisée dans les processus décisionnels concernant les individus plutôt que des actions de surveillance.

---

[9] André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n^{o} 19.

4. Une fuite en avant : de la vie privée à la « vie personnelle »

Un très grand nombre d'usages d'informations personnelles ne sont pas une violation de la vie privée. Il est difficile de justifier, au nom de la vie privée, les mesures relatives à certaines informations dont la circulation est inhérente à la vie sociale. C'est probablement pour cette raison que certains se sont rabattus sur une notion extrêmement vague et d'une ampleur encore indéterminée : la notion de vie personnelle. Cette notion semble résulter d'une tentative de pallier aux difficultés conceptuelles découlant de la fragilité des fondements sur lesquels reposent les mesures de contrôle des informations personnelles ne se rattachant pas à la vie privée.

La crainte que les informations soient utilisées de manière inadéquate porte à rechercher une protection pour toutes les informations relatives à une personne. Dès lors que l'on postule qu'il n'y a pas d'informations anodines, que le couplage peut permettre de dresser des profils à partir des traces les plus banales, on ne peut plus faire la distinction entre les informations relevant du domaine public et celles qui relèvent de la vie privée. Il devient du coup plus difficile d'asseoir les fondements des régimes de protection des données personnelles uniquement sur un souci de protéger la vie privée. Étant donné les perceptions des risques susceptibles de découler de recoupements d'information, on en est venu à trouver naturel que le droit sanctionne toute circulation d'information a priori, sans égard à la faute, sans égard au fait que la vie privée des personnes ait été ou non violée, ou qu'un dommage ait été effectivement causé.

D'où cette revendication pour la reconnaissance d'un « droit à la vie personnelle ». Par exemple, Frayssinet fait valoir que « l'atteinte ne concerne pas que la vie privée (…) mais tous les aspects de la vie personnelle »[10].

---

[10] Jean FRAYSSINET, « La protection des données personnelles est-elle assurée sur Internet ? », Texte présenté au colloque international *Droit de l'Internet, approches européennes et internationales*, septembre 2001, http://droit-internet-2001.univ-paris1.fr/pdf/vf/Frayssinet.pdf. Voir aussi André LUCAS, Jean DEVEZE et Jean-FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 50.

Il en résulte une kyrielle de revendications ayant l'apparence d'une quête généralisée d'un droit de veto à l'égard de toutes les informations sur les personnes, y compris celles qui étaient il n'y a pas si longtemps perçues comme relevant des inconvénients normaux de la vie en société. Par exemple, on invoque le droit de ne pas recevoir des dépliants publicitaires etc. ou de sollicitations par courriel. Ces craintes, en partie justifiées, entraînent des revendications pour mettre en place des contrôles à l'égard de toutes sortes de situations mettant en cause des informations personnelles. À bien des égards, les revendications pour renforcer la protection des données personnelles sont parfois devenues des revendications pour protéger d'inconvénients inhérents à la vie sociale, non pour assurer la protection de la vie privée. C'est une approche incompatible avec les exigences d'une société démocratique car elle nie l'exercice des autres droits fondamentaux comme la liberté d'expression ou les exigences d'imputabilité.

La notion de « protection de la vie personnelle » ne comporte pas de contours définis; elle paraît pour l'essentiel renvoyer aux préférences des individus. Il est difficile de voir où s'arrête une telle notion. Si la notion veut dégager une aire de protection afin d'assurer l'intimité des individus de même que la possibilité d'exercer un contrôle sur leur vie, elle se confond avec la notion de vie privée, une notion toutefois délimitée par les impératifs de la vie en société. Si la notion de « vie personnelle » va plus loin que le droit à la vie privée pour ériger au rang de droit tout ce qui, au fil de leurs sensibilités, peut déranger les personnes, la notion n'est reconnue nulle part dans des lois ou les textes constitutionnels. Il serait dangereux de fonder un droit sur une notion aussi tributaire des sensibilités variables, voire arbitraires des individus.

Au surplus, la notion de « vie personnelle » laisse peu de place aux impératifs de la vie en société, au fait que l'information doit pouvoir circuler au nom d'intérêts de la collectivité et que cette circulation, en pratique, est rarement préjudiciable. Si tout n'est qu'affaire de choix individuels, il reste peu de place pour la circulation de l'information qui répondrait à des impératifs de la collectivité.

Enfin, si toutes les activités humaines significatives supposent désormais l'usage des réseaux, il faudra bien convenir qu'il faut un cadre juridique suffisamment nuancé pour assurer les équilibres entre les divers droits mis en cause dans les interactions sociales. Dans ce contexte, la notion de « vie personnelle » paraît trop rudimentaire pour servir de cadre

de réflexion. Pire encore, par la négation des autres valeurs inhérentes à la démocratie qu'elle comporte nécessairement, la notion recèle une tendance au recul de l'état de droit.

Ce genre de dérive emporte une importante distraction de ressources vers la protection des désirs individuels relevant habituellement du caprice alors qu'elle laisse le champ libre à des pratiques autrement plus attentatoires à la vie privée. Au nom de cette notion, on multiplie les précautions afin de censurer des informations à caractère public alors que peu est fait pour encadrer les activités de surveillance, notamment par les agences privées d'investigation ou d'évaluation du crédit des particuliers.

Par exemple, au Québec, une entreprise qui collecte et diffuse à ses membres des renseignements sur le crédit des particuliers est l'objet de plusieurs poursuites à chaque année sans que cela ait apparemment suscité l'attention de la Commission d'accès à l'information. Pourtant, cette dernière s'est inquiétée des dangers de la recherche généalogique et n'a pas manqué de mettre de l'avant des scénarios catastrophes à l'égard de plusieurs projets d'implantation de fonctionnalités destinées à faciliter les transactions en ligne entre le gouvernement et les citoyens. On peut s'étonner d'un tel zèle à l'endroit de projets qui semblent conçus de manière à assurer un haut degré de respect de la vie privée et un apparent désintérêt pour les activités d'entreprises qui ne semblent pas mettre beaucoup d'efforts afin d'assurer la qualité des informations qu'elles diffusent à l'égard du crédit des citoyens.

B) Une application de plus en plus laborieuse

La protection des données personnelles a donné lieu à un ensemble de dérives conceptuelles qui ont rendu son application de plus en plus laborieuse. Les dysfonctionnements sont encore plus visibles dans les situations où l'information doit circuler pour assurer le déroulement d'activités sociales menées généralement dans l'intérêt même des individus vivant en société.

1. L'illégitimité des espaces publics

La portée étendue conférée à la notion de données personnelles a parfois conduit à transformer des informations ayant un caractère public

en des données devant être traitées comme si elles étaient confidentielles. Ces démarches procèdent d'une négation de l'équilibre que plusieurs systèmes juridiques avaient pourtant pris soin de ménager entre les impératifs de protection de la vie privée et la nécessité de laisser circuler certaines informations relatives aux personnes. Les exemples suivants tirés de l'application de la législation québécoise illustrent cet inquiétant phénomène.

Par exemple, au Québec l'article 55 de la Loi d'accès[11] précise « qu'un renseignement personnel qui a un caractère public en vertu de la loi n'est pas nominatif. » Au départ, il est ici question de renseignements régis par un principe de libre de circulation. En dépit de cela, la Commission d'accès à l'information, chargée de l'application du volet protection des données personnelles de la Loi n'a pas hésité à imposer des limites à la circulation de renseignements que le législateur a pris le soin de soustraire au régime des renseignements nominatifs.

Un Avis de la Commission québécoise chargée de l'application des lois sur la protection des données personnelles portant sur les infrastructures à clés publiques[12] illustre l'ampleur de la dérive. L'Avis consultatif ne tient pas compte du caractère public[13] des informations consignées dans un répertoire associé à une infrastructure à clé publique. L'Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementales du secrétariat du Conseil du Trésor affirme péremptoirement que « L'utilisation d'ICP implique pour les individus et organisations une cueillette d'informations additionnelles et une surveillance de leurs actions » (nous soulignons). Qu'il existe des risques pour la protection de la vie privée résultant de ce genre d'infrastructure est évidemment possible. Mais de poser a priori que la surveillance est une conséquence découlant nécessairement de l'utilisation d'une ICP relève du domaine de l'affirmation gratuite.

---

11 *Loi sur l'accès aux documents des organismes publics et sur la protection des données personnelles*, L.R.Q., c. A-2.1, ci-après citée Loi sur l'accès.

12 COMMISSION D'ACCÈS À L'INFORMATION, *Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du secrétariat du Conseil du trésor*, août 2001, < http://www.cai.gouv.qc.ca/fra/docu/a011107.pdf >

13 L'article 50, 2e al. de la *Loi concernant le cadre juridique des technologies de l'information* affirme le caractère public du répertoire.

Dans son Avis relatif à la diffusion sur Internet de renseignements contenus dans les demandes de permis de construction[14], la Commission prend sur elle de restreindre la notion de renseignements à caractère public au motif, pourtant non prévu dans la loi, que ces renseignements à caractère public une fois sur Internet pourraient devenir accessibles à des millions d'Internautes et que cela pourrait faire du Québec « un paradis du marketing direct. » On peut certes en avoir contre le marketing direct et trouver désagréable de recevoir des publicités non-sollicitées. C'est, à ce jour, matière de préférences personnelles. L'activité de marketing direct n'est pas illégale au Québec. Il est surprenant qu'un organisme public chargé d'appliquer la loi se permette de poser de tels jugements de valeur au sujet d'une activité en elle-même licite.

De plus, la Commission impose des obligations relativement à la finalité des informations à caractère public. Elle affirme que « même si la loi est muette à ce sujet, on peut tout de même cerner l'objectif visé par une telle disposition. » Elle ajoute ainsi à la loi en y incluant une sorte de limite intangible au caractère public des renseignements fondée sur leur finalité supposée. Ce procédé est très inquiétant : on se met ainsi à poser des jugements de valeur au sujet de tout un ensemble possible d'usages d'informations publiques. Consulter le rôle d'évaluation pour prendre connaissance du fait que telle ou telle personne possède tant d'immeubles dans une ville est-il illégitime ? Il n'y a rien qui décrète que le fait qu'une personne soit propriétaire d'un immeuble, voire de plusieurs, relève de sa vie privée. Par contre, le droit sanctionne déjà — et à juste titre — la diffusion abusive de telles informations lorsque cela résulte d'un geste malveillant ou que l'intérêt public ne justifie pas.

Les craintes à l'égard de possibles usages abusifs de données publiques conduisent à l'imposition de restrictions drastiques des possibilités d'accéder à des renseignements en se fondant sur les finalités, réelles ou supposées sous-jacentes à leur caractère public. Les informations à caractère public sont ainsi censurées au motif qu'il existe des risques — le plus souvent hypothétiques — que certaines d'entre elles soient utilisées de manière fautive.

---

[14] COMMISSION D'ACCÈS À L'INFORMATION, *Avis relatif à la diffusion via intranet et Internet par la ville de Gatineau des renseignements contenus dans les demandes de permis de construction, mai 1999*, < http://www.cai.gouv.qc.ca /fra/docu/a990534.pdf >

Cette dérive a même été reprise dans la Loi concernant le cadre juridique des technologies de l'information[15]. Cette loi impose un mécanisme de censure des documents publics comportant des données personnelles. L'article 24 de cette loi se lit comme suit :

> L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des données personnelles et qui, pour une finalité particulière est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut, en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 68, fixer des conditions pour l'utilisation de ces fonctions de recherche.

Cette disposition vise des informations qui ont un caractère public; elle ne concerne pas les renseignements à caractère privé. Elle permet de restreindre l'utilisation des fonctions de recherche extensive à l'égard des documents technologiques comportant des données personnelles et rendues publiques pour une finalité particulière. On veut ainsi éviter, par exemple, les consultations de banques de données à l'aide de moteurs de recherche afin de repérer des données personnelles pour des fins autres que celles pour lesquelles elles ont été recueillies ou diffusées.

On peut supposer que ce genre de mesure se justifie du fait que dans l'univers des documents sur papier, la recherche est souvent longue puisque les documents publics doivent être examinés un à un. Pour les documents technologiques, les possibilités de recherche sont démultipliées, ce qui peut laisser craindre des abus. Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des données personnelles contenus dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées. Les décideurs vont devoir se mettre à spécifier les finalités du caractère public d'une information. Il est difficile de concevoir comment une telle démarche est possible sans

---

[15] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, < http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html >.

porter un jugement a priori sur la légitimité de certaines recherches; sans parler de la difficulté de déterminer, en l'absence de texte législatif, ce qui constitue la finalité du caractère public d'une information. En fait, lorsqu'une information est à caractère public, elle est de libre parcours, sauf à démontrer qu'on en fait un usage fautif ou contraire à une loi. On ne peut présumer, sans nier le caractère public d'une information, qu'une information ne doit servir qu'à certaines fins et pas à d'autres. La seule limite légitime à l'usage d'une information à caractère public est le caractère abusif de l'usage : postuler a priori que des usages seraient abusifs laisse fort peu de place au droit à l'information.

Avec ce genre d'approche il n'y a plus d'informations à caractère public : il n'y a que des informations qui peuvent circuler pour des fins prédéterminées par les autorités publiques ou privées et ce, au gré de procès d'intention sur de possibles usages malveillants. On a peine à croire que cette approche ait été retenue au Québec qui a pourtant été l'un des premiers à proclamer, à l'article 44 de la Charte des droits et libertés de la personne le droit à l'information,. Les valeurs au nom desquelles certaines informations ont un caractère public sont ignorées. Seuls semblent compter les dangers, généralement hypothétiques, qui pourraient exister pour la protection de la vie privée. Le biais est troublant et profondément incompatible avec l'idée selon laquelle tous les droits et libertés connaissent des balises découlant de l'exercice d'autres droits.

Une autre faiblesse de ces analyses tient au fait qu'elles prennent peu d'intérêt pour l'analyse des alternatives aux mesures préconisées qui sont invariablement de retrancher des informations du domaine public au gré de demandes fondées sur des appréhensions discutables. D'une part, on prête des finalités déterminées à des renseignements qui sont de libre parcours sous réserve d'abus et on postule qu'un renseignement ne peut avoir qu'une finalité fixe. Ces approches révèlent une rigidification à l'égard de la notion de finalité.

2. La rigidification du principe de finalité

Le principe de finalité pose que l'on ne peut recueillir et utiliser l'information que pour des fins compatibles avec celles de la collecte initiale. La rigidité donnée au principe a contribué à immobiliser l'information personnelle. On a eu tendance à en faire un principe limitant les usages possibles de ces informations personnelles. Cela a eu souvent

pour conséquence de forcer à la redondance : il faut redemander et redemander les mêmes informations car celles qui sont disponibles ont été recueillies pour d'autres fins.

Pourtant, le principe de finalité procède d'un souci de maintenir la qualité de l'information. Le principe est ainsi exprimé par l'OCDE :

> Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.[16]

Une information peut très bien convenir pour répondre à un besoin. Elle sera inadéquate, voire franchement contre-indiquée, pour répondre à un autre type de besoin. Dans l'univers des réseaux où l'information est persistante et circulante, il importe de revenir aux fondements véritables du principe de finalité. Il s'agit d'assurer que les informations utilisées sont de qualité adéquate pour servir aux fins envisagées, non ériger la redondance en garantie de la vie privée !

Lucas, Devèze et Frayssinet rappellent ainsi la raison d'être du principe de finalité :

> Plus que la nature ou la signification première de l'information ou de la technique utilisée, le danger est dans les finalités des usages des données personnelles. La finalité doit être légitime pour le gestionnaire des informations, utile ou nécessaire pour la personne concernée qui a besoin d'information préalable, d'une capacité de choix éclairé et personnel pour déterminer son autonomie informationnelle.[17]

---

[16] OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, < http://oecdpublications.gfi-nb.com/cgibin/OECDBookShop.storefront/EN/product/932002012P1 >

[17] André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 11.

D'un principe conçu pour procurer des balises au droit de traiter des informations personnelles obtenues d'une personne, on en a fait un principe justificatif de la censure imposée à la circulation des informations. Au nom des possibles et hypothétiques détournements d'informations sur des personnes, on a construit un régime de contrôle des informations afin de les soustraire aux usages non-prévus initialement et les assujettir, comme si ces informations relevaient de l'intimité, à un droit de veto des personnes ou des bureaucraties.

Le principe de finalité est né d'une démarche où il s'agissait principalement de sanctionner après-coup des usages abusifs. Il trouvait application une fois que l'on avait constaté que des informations étaient utilisées et que se posait la question de savoir si cela correspondait bien aux fins pour lesquelles le renseignement avait été recueilli. On a fait de ce principe une règle s'appliquant a priori même aux renseignements ayant un caractère public.

Pourtant, le principe de finalité n'a de sens que dans le cadre d'une évaluation du caractère fautif de l'utilisation d'une information. Il y a en effet de sous-jacent aux interdits de changement de finalités, un souci de prévenir les changements significatifs et préjudiciables dans les usages des informations. Dans un monde d'informatique centralisée ou l'usager n'a pas accès, il faut un moyen afin de garantir que des informations équivoques ne seront pas utilisées afin de prendre des décisions. Ce qui est problématique dans l'utilisation d'une information pour des finalités différentes de celles pour lesquelles elle avait été recueillie, c'est le risque que cette information soit de piètre qualité pour les nouvelles fins auxquelles on souhaite l'utiliser. Faute d'une volonté de promouvoir des moyens afin de garantir que l'information utilisée pour prendre des décisions relatives à une personne sera de qualité, on en est venu à interdire les changements de finalité.

Face aux risques que les informations utilisées pour une prise de décision soient inadéquates, on doit envisager de renforcer les mécanismes tendant à assurer la qualité de l'information plutôt que d'en empêcher platement la circulation. Le contrôle de finalité doit par conséquent être envisagé comme un contrôle de qualité : à chaque fois qu'on utilise une information, il faut la valider au regard des décisions pour lesquelles on entend l'utiliser. Dans plusieurs situations, cela peut se faire en présentant l'information à la personne concernée et lui demander de la valider et le cas échéant de la rectifier.

Mais plutôt que de promouvoir le développement d'exigences tendant à l'amélioration de la qualité des données, on tombe souvent dans le recours machinal au consentement : un procédé qui porte à se dispenser de faire les efforts afin d'assurer la qualité de l'information.

3. Le recours machinal au consentement comme palliatif à la rigidité

C'est au prix de contorsions et d'artifices que l'on parvient à concilier la conception classique de la protection des données personnelles avec les exigences du fonctionnement réaliste des environnements d'information. Parmi les contorsions les plus apparentes, il y a celles auxquelles a donné lieu la pratique relative au « consentement libre et éclairé. »

Au Québec, la Commission a subordonné la divulgation de données personnelles au consentement manifeste, libre, éclairé, donné à des fins spécifiques par la personne concernée. Pourtant, l'exigence mentionnée dans la Loi sur la protection des données dans le secteur public est celle d'une autorisation, qui pourrait être implicite ou simplement découler du contexte. Cette exigence de consentement et la lourdeur qui l'accompagne est devenue une exigence fondamentale dans le cycle de gestion des données personnelles. L'effet pervers de ce genre de dérive est de faire porter les efforts sur la recherche et la gestion du consentement plutôt que sur la protection effective de la vie privée des personnes.

L'obligation d'obtenir le consentement libre et éclairé servait à l'origine à baliser le droit de procéder à des interventions médicales. En l'important dans le champ de la protection des données personnelles le procédé a induit une rigueur à l'origine conçue pour encadrer les interventions pouvant avoir des conséquences infiniment plus drastiques ! Les exigences au sujet du caractère libre, éclairé, non équivoque et consigné par écrit pouvaient fort bien se comprendre lorsqu'il s'agit de porter atteinte à l'intégrité physique d'une personne. Est-ce adapté aux transferts d'informations, dont plusieurs sont effectués dans l'intérêt même du citoyen ?

L'exigence de consentement a engendré un dysfonctionnement particulièrement visible lorsque vient le temps de penser la circulation de l'information dans les réseaux. Pour contourner la difficulté découlant du

caractère excessivement englobant de la notion de données personnelles, on a vu se développer des pratiques fondées sur une véritable mythologie du consentement « libre et éclairé ». On en vient à se demander si les ressources qu'on se croit obligé de consacrer à la gestion des consentements ne seraient pas mieux investies dans une gestion plus serrée des informations personnelles, en fonction des risques.

En France, la CNIL relève les malentendus que la généralisation des recours au consentement pourrait introduire dans la gestion de l'information par les organismes publics. Dans son 22e rapport d'activités 2001, la Commission écrit : « Promouvoir le consentement ne risque-t-il pas de donner à croire que chacun serait libre de ne pas figurer dans un fichier fiscal, un fichier de police, un fichier de gestion administrative ? Ce serait tromper nos concitoyens sur la réalité de leurs droits et peut-être sur l'essentiel de ce qui constitue le lien social qui contraint à devoir concilier vie privée et d'autres valeurs d'intérêt général […] ». Et la CNIL d'ajouter qu'« en sens inverse, promouvoir le consentement, ne peut-il aboutir à anéantir des garanties d'intérêt public au motif que les personnes auraient consenti ? »[18].

Ces dérives autour de la notion de consentement sont révélatrices du fait que, bien souvent, on a perdu de vue la raison d'être de la protection des données personnelles. D'une finalité de protéger la vie privée on est passé à celle de donner suite à un plus ou moins mythique « droit de veto » de la personne sur les informations la touchant. Le consentement, qui était au départ un moyen d'assurer au sujet la maîtrise nécessaire sur les renseignements relevant de sa vie privée, est devenu une fin en soi, quitte à ce qu'il soit perverti ou banalisé afin de contourner les rigidités résultant d'une conception trop englobante de la protection des données personnelles. C'est ainsi que s'est répandu sur Internet, la pratique de requérir de l'usager qu'il consente…. à toutes sortes d'usages dans des contrats que personne ne prend le temps ou n'a le courage de lire. Le droit de la protection des données a été ramené à une simple obligation d'exiger un clic de la part de l'usager ! Voilà bien une démonstration de

---

[18] Commission nationale de l'informatique et des libertés, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108 et 109, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf >

l'inefficacité de cette approche formaliste qui repose sur le mythe du consentement soi disant libre et éclairé.

4. La multiplication des lois d'exceptions

La rigidité de l'application des règles en matière de protection des données personnelles de même que l'extension excessive de certaines notions ont rompu l'équilibre. C'est sans doute pour cette raison que les législateurs se trouvent de plus en plus dans l'obligation d'intervenir au moyen de lois afin de rétablir les équilibres rompus en matière de protection des données personnelles. Herbert Burkert constate que dans plusieurs pays, se sont multipliées les lois d'exception, venant sectoriellement restreindre ou baliser le droit à la protection des données personnelles. Il écrit qu' :

> Il est en effet qu'à considérer l'ensemble des textes législatifs émis depuis la promulgation des premières lois sur la protection des données, pour se rendre compte qu'ils comportent une multitude de textes sectoriels. Tous ne prennent pas la forme de lois spéciales; certains se présentent sous forme de simples amendements ou compléments. Cette législation, et tout particulièrement celle relative au traitement des données détenues par le secteur public, a globalement limité la portée des principes généraux en la matière en introduisant ce que l'on a vu comme des compromis entre le respect de la vie privée et les nécessités de l'intérêt public. Et s'il est vrai que les individus sont attachés au respect de leur vie privée, ils s'en détachent rapidement dès lors qu'ils sont appelés à choisir entre confidentialité et sécurité- qu'il s'agisse de sécurité sociale ou publique.[19]

Cette tendance à la multiplication de lois venant apporter des ajustements sectoriels au droit de la protection des données personnelles est un indice du caractère inadéquat des mécanismes généraux. Le cadre juridi-

---

[19] Herbert BURKERT, « Progrès technologiques, protection de la vie privée et responsabilité politique, 89 *Revue française d'administration publique*, janvier-mars 1999, pp. 119-129, p. 125.

que général de la protection est trop rigide, ou perçu comme tel pour accommoder les autres impératifs. Pour illustrer l'ampleur de la dérive à laquelle on doit remédier, rappelons qu'au Québec, une loi a été adoptée afin de permettre la circulation d'informations de manière à rendre possible les mesures de prévention des suicides ou autres actes de violence contre une personne identifiable[20]. Cette loi a ajouté l'article 59.1 à la Loi d'accès prévoyant que :

> Un organisme public peut communiquer un renseignement nominatif, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide lorsqu'il existe un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable.

Que l'on en soit venu à une telle solution pour rendre juridiquement possible ce qui aurait été, dans une interprétation raisonnable et nuancée de la loi, un motif légitime de donner accès à des informations personnelles montre la rigidité des conceptions du droit de la protection des données personnelles. Jusqu'à cet amendement, la protection des données personnelles était lue de manière à faire prévaloir la protection des renseignements relatifs à une personne même à l'encontre de la protection de la vie !

II- Pistes pour renforcer la protection de la vie privée dans les réseaux

Devant les carences que présente le droit relatif à la protection des données personnelles, il faut identifier des voies qui permettront une mise à niveau avec les impératifs contemporains de meilleure circulation de l'information tout en renforçant le niveau de protection de la vie privée des personnes. Il est nécessaire d'actualiser les mécanismes de protection des droits des personnes afin d'assurer une protection effective de la vie

---

[20] *Loi modifiant diverses dispositions législatives eu égard à la divulgation de renseignements nominatifs en vue d'assurer la protection des personnes*, L.Q., 2001, c. 78. < http://publicationsduquebec.gouv.qc.ca/fr/cgi/telecharge.cgi/180F0206.PDF?table=gazette_pdf&doc=180F0206.PDF&gazette=4&fichier=180F0206.PDF >

privée. Une telle démarche doit être menée selon une approche assurant à la fois une réelle protection de la dignité des personnes et la libre circulation des informations relevant de l'espace social.

L'accélération de la circulation des informations et les conséquences qui en résultent appellent des modalités conséquentes au plan des encadrements normatifs. L'instantanéité des activités dans les réseaux s'oppose de plus en plus à la valorisation de la stabilité et du conformisme si cher à certaines communautés bureaucratiques. Cette accélération appelle la conception de cadres normatifs reflétant cette vélocité de l'information, non des normes pour figer l'information sous le prétexte de la protéger.

La généralisation des plates-formes de partage d'informations met à la portée de tous un ensemble de possibilités d'échange et de diffusion d'informations. Pour l'information qui est en possession de l'Administration, le cadre juridique devrait s'attacher à en régir les conditions d'accès par chaque agent de l'État plutôt que d'en interdire la circulation. Dans un pareil contexte, l'enjeu n'est plus de savoir si une donnée peut ou non être en possession de l'Administration mais plutôt si cette dernière a le droit d'y accéder et d'en faire usage pour prendre une décision dans chaque situation spécifique.

A) Une lecture actualisée des principes de protection des données personnelles

Dans un monde en réseau, les informations sont essentiellement circulantes : il faut qu'elles soient disponibles au moment où elles doivent l'être pour accomplir une prestation de service. Il faut recentrer les fondements de la protection des données personnelles en fonction de la vélocité accrue découlant des réseaux numériques et autres environnements d'information.

Les principes fondamentaux du droit de la protection des données personnelles composent la structure d'instruments internationaux de protection des données personnelles comme les Lignes directrices de

l'OCDE,[21] la Convention européenne et la Directive de la Commission européenne, mais également de plusieurs législations nationales[22].

Dans un environnement en réseau, la nécessité de la collecte doit s'envisager au regard de l'ensemble des familles de prestations concernées par les informations. Une fois l'information collectée, la nécessité de sa conservation s'apprécie au regard d'un ensemble de processus de décision. Le principe de retenue en matière de collecte et le principe de spécification des finalités se recoupent. Le principe relatif à la spécification des finalités est aussi renforcé: en spécifiant le plus strictement possible les finalités, on se trouvera en situation où la collecte est limitée aux informations effectivement indispensables aux fins poursuivies au plan de l'ensemble des prestations et services devant être assurés au sein d'un réseau.

La règle empêchant la circulation et la réutilisation des informations pour le motif que celles-ci pourraient être détournées de leur finalité, doit être relue dans le contexte de dialogue accru que permet le réseau. Plus que jamais, l'Administration est en mesure d'indiquer à chaque administré quelles sont les informations qu'il possède sur son compte, lesquelles il entend utiliser afin de prendre une décision. Le citoyen est désormais en mesure d'interagir et d'exiger le retrait et l'ajout d'informations.

La généralisation des réseaux conduit à apprécier la nécessité à l'égard de l'ensemble des situations concernées par un environnement d'information. Certes, il faut toujours considérer la nécessité au plan de la légitimité de la collecte et de la détention d'informations, comme cela est exigé par les principes actuels. Mais il faut assurer que seules les informations pertinentes et autorisées sont utilisées dans le cadre d'un processus décisionnel spécifique. Cela appelle une démarche dans laquelle sont dissociées, d'une part, la question de la nécessité de la détention de l'information et, d'autre part, l'appréciation de la nécessité d'y accéder pour une décision ou prestation déterminée.

---

21 OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, http://www.oecdpublications.gfi-nb.com/cgibin/OECDBookShop.storefront/EN/product/932002012P1.

22 L.R.Q., c. P-39.1.

La limitation en matière de collecte suppose la mise en place de processus décisionnels qui feront usage du minimum d'informations personnelles nécessaires afin d'assurer les prestations ou la prise de décision. Il faut être en mesure de justifier le pourquoi de la collecte de chaque renseignement personnel.

Le principe de finalité pose que l'on ne peut recueillir et utiliser les renseignements personnels que pour des fins compatibles avec celles de la collecte initiale. Le principe de finalité est lié au maintien de la qualité de l'information. Dans les principes de l'OCDE, cette exigence est ainsi exprimée :

> Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.[23]

Dans le contexte d'un environnement en réseau, la question des finalités se pose en tenant compte que les informations peuvent être là disponibles, déjà recueillies : ce n'est plus au regard de la détention que s'applique l'exigence du respect de la finalité mais plutôt au regard de l'accès et de l'utilisation du renseignement. Dans un réseau, le principe du contrôle au niveau du droit d'accès vient assurer le respect des finalités. L'accès à un renseignement n'est licite que pour une finalité autorisée et lorsqu'on accomplit une activité s'inscrivant dans le cadre de la finalité.

Le respect du principe de finalité, suppose que l'usager ait effectivement connaissance des familles de finalités auxquelles serviront les informations. Il faut que l'information sur les finalités des informations détenues soit constamment disponible et portée à la connaissance de l'usager lors de chaque collecte. Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale.

---

[23] OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, <http://www.oecdpublications.gfinb.com/cgibin/OECDBookShop.storefront/EN/product/ 932002012P1.

La transparence est une condition essentielle de la crédibilité et de la confiance dans les environnements en réseau. L'usager doit être en mesure de savoir à qui il a affaire et comment est conçu le processus informationnel dans lequel il est engagé. À cet égard, l'évaluation publique des environnements d'information ou des partages d'informations à des fins de prestations électroniques prend une importance accrue. Les enjeux et les risques associés à des prestations électroniques que l'on projette de proposer en réseau doivent être publiquement divulgués, débattus et leurs risques publiquement évalués.

La qualité des données s'apprécie à l'égard des prestations à être accomplies avec les renseignements : il faut garantir que les renseignements utilisés pour effectuer la prestation sont exacts, précis, autorisés par les lois et ne présentent pas d'équivoque. La légitimité de pareilles circulations d'informations personnelles est renforcée lorsque le citoyen se trouve à même de réviser et, le cas échéant, de rectifier en ligne ou autrement les informations personnelles. Le droit de rectification - pour l'heure si peu utilisé- prend alors tout son sens.

Comme les données personnelles sont disponibles en réseau, le cadre juridique doit obliger les prestataires à s'assurer que l'information à laquelle ils accèdent, afin d'accomplir une prestation relative à une personne, est de qualité adéquate, compte tenu des exigences et du contexte de la prestation. Pour assurer la qualité, il faut tabler sur le potentiel de dialogue en direct que recèlent les technologies de réseau.

À cet égard, le principe de la participation individuelle de la personne concernée dans les décisions relatives au traitement des renseignements personnels acquiert dans les réseaux une portée renouvelée. Dans les réseaux, il est possible de présenter l'information que l'on possède et de la valider en temps réel avec la personne concernée. La garantie de la qualité des données sera du même coup renforcée par la validation que l'organisme effectue de l'information lors d'une prestation spécifique.

S'agissant de la responsabilité, chaque entité susceptible d'accéder à des données personnelles au sein d'un réseau peut être considéré comme en étant le détenteur juridique. À ce titre, il est responsable de la confidentialité. Il importe à cet égard de préciser les obligations et délimiter la responsabilité des gestionnaires quant aux exigences de confidentialité et de sécurité. Il est en effet nécessaire que soient précisées les normes à la

lumière desquelles seront évaluées le comportement et la responsabilité des citoyens de même que celle du gestionnaire.

La sécurité tant physique que logique est évidemment une exigence essentielle pour tout environnement fonctionnant en réseau. Le cadre juridique doit inciter les responsables à prendre les mesures afin de garantir la sécurité des informations sur les personnes. Outre une culture de la sécurité, il faut un ensemble de processus capables de prévenir les attaques et surtout d'y remédier aussitôt que se produit un évènement qui met en péril les processus de traitement.

B) L'impératif de confiance

Tout au long du cycle de traitement de l'information, il faut garantir un environnement dans lequel l'usager/citoyen est en confiance. Les traitements doivent se faire en pleine transparence. En informant l'usager de ce qu'il advient de l'information qu'il confie à l'État, on tisse un lien de confiance. Plus les informations sont sensibles, plus il faut multiplier les précautions afin de garantir le niveau de confiance conséquent. Lorsque des garanties sont données, il faut impérativement que des mesures appropriées en assurent le respect.

La mise en en place de l'environnement en réseau doit découler d'un processus public d'évaluation des enjeux et des risques. Pour procurer la légitimité et la confiance essentielle à l'acceptabilité des modes de circulation de données personnelles, il importe que tous les enjeux, toutes les appréhensions soient pris en considération. Les questions que se posent les citoyens doivent reçevoir des réponses.

Christine Noiville écrit que la prise de décision à l'égard de phénomènes comportant des risques à être assumés par la collectivité doit comporter une dimension explicative et délibérative. Elle écrit :

> Rappelons-le : un risque n'est pas en soi acceptable, il le devient par le prisme du débat, qui lui donne sa légitimité. L'acceptabilité n 'est pas une essence qui s'imposerait à celui qui est confronté au risque. [...] Ainsi, parce que le « risque acceptable » n'est pas un « donné » mais le fruit d'une appréciation à chaque fois renouvelée, le sens qu'il

> convient de lui attribuer doit autant que possible être négocié.[24]

La mise en place d'environnements d'information où sont traités des renseignements personnels présente des enjeux semblables à ceux qui se présentent lorsqu'on s'interroge sur les impacts environnementaux d'un projet. On s'inquiète des précautions qui ont été prises, des conséquences non prévues, des problèmes particuliers que pourraient vivre certaines personnes. On veut être rassuré à l'égard des précautions, des analyses d'impacts et des mesures de contrôle qui préviendront les possibles dérives.

Pourtant, les organismes publics promoteurs de projets anticipent ces préoccupations et ont à cœur de concevoir des services et des prestations qui assurent un niveau élevé de protection. Le processus public permet de porter ces précautions à la connaissance publique. Il permet un débat éclairé sur les choix à faire et un regard critique sur les choix qui ont été faits.

C) Le droit à une technologie compatible avec la protection de la vie privée

La protection effective de la vie privée appelle le développement d'un droit à ce que soient mis en place des environnements technologiques qui accroissent la protection de la vie privée plutôt que de la diminuer. Les décideurs publics et les entreprises privées pourraient se voir imposer l'obligation de démontrer que la technologie mise en place répond à des exigences minimales de protection de la vie privée. Pour y arriver, il faudrait qu'il existe une obligation de planifier la mise en place de technologies en tenant compte des dimensions juridiques. Ce n'est pas toujours ainsi que sont planifiés les systèmes d'information. Très souvent, les environnements d'information sont développés sans se soucier des dimensions juridiques et présentés ensuite comme une sorte de situation inévitable à laquelle il faut s'adapter. S'il est un domaine où le droit devrait

---

[24] Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, « Les voies du droit », 2003, p. 120.

jouer un plus grand rôle, c'est au niveau des balises lors du développement d'environnements d'information.

La sécurité n'égale pas automatiquement protection de la vie privée. L'on convient sans peine que la protection de la vie privée suppose que les informations et les systèmes soient dotés des caractéristiques assurant la sécurité physique et logique des informations. Mais la protection de la vie privée requiert des démarches allant largement au-delà de celles qui sont nécessaires afin de sécuriser un système d'information ou un réseau.

L'emploi des technologies de l'information modifie l'échelle des risques associés à la circulation des informations. Ce phénomène requiert une démarche d'évaluation des risques, non de prendre pour acquis le pire des scénarios afin de déterminer le niveau de protection que la loi devrait exiger. Ceux qui mettent en place des environnements technologiques devraient avoir l'obligation de démontrer que ceux-ci fonctionnent dans le respect de la vie privée, entendue comme protégeant la dignité. En particulier, il n'y a pas de raison pour qu'il incombe aux personnes de prendre les moyens et faire les démarches pour assurer le respect de leur vie privée : le devoir de protéger la vie privée des personnes est plus facile à assumer au niveau de la mise en œuvre et du déploiement des environnements. Cela est particulièrement vrai dans les environnements voués au service public.

Mais cela nécessite la mise en place d'un processus cohérent d'évaluation préalable des systèmes. Une telle évaluation ne devrait pas se fonder sur des scénarios catastrophes mais devrait plutôt avoir pour finalité de vérifier si les choix ont été effectués de manière à respecter les principes énoncés dans les principes reconnus. Par la suite, lorsque sont signalées des situations attentatoires à la vie privée, un processus d'enquête devrait viser à documenter les incidents et prescrire les correctifs afin d'éviter qu'ils se reproduisent.

D) La maîtrise des données personnelles

La protection de la vie privée et des informations personnelles suppose de reconnaître à la personne concernée un droit d'exercer un certain contrôle sur ce qu'il advient des renseignements la concernant. Mais ce droit de contrôle n'a jamais été et ne saurait être absolu. Lucas, Devèze

et Frayssinet rappellent qu'« il n'y a pas de vie sociale sans échanges de données personnelles ». Ces auteurs ajoutent qu'« une personne est non seulement un être physique et psychique mais aussi un être informationnel (…). » Il faut donc poser le principe en convenant de ses limites. Le rapport Truche rappelle que « le principe de maîtrise des données personnelles ne saurait être posé en absolu »[25]. La CNIL exprime aussi des réserves au sujet d'un droit de maîtrise des données personnelles en rappelant que ce qui est essentiel, c'est que les données soient de qualité. Dans son 22e rapport d'activité, la CNIL écrit que :

> Mais ne peut-on soutenir que si le droit d'accès est peu exercé, en pratique, c'est qu'au fond l'essentiel pour nos concitoyens n'est pas tant de vérifier la teneur des données qu'ils ont le plus souvent communiquées eux-mêmes à l'administration concernée, que d'avoir la garantie que ces données ne seront pas détournées de la finalité initiale, communiquées à des tiers qui n'ont pas à en connaître ou leur serait opposables de nombreuses années après.[26]

Le droit de contrôle des données peut être conçu comme un droit s'exerçant a priori. Il peut aussi s'exercer a posteriori, lorsqu'un usage inadéquat a été fait d'une information et qu'il convient de le rectifier. Ainsi un droit de contrôle a priori peut être exercé par la personne concernée à l'égard de toutes les informations personnelles détenues sur elle-même. Il devrait être possible d'exercer rapidement un recours en accès et rectification et demander des correctifs. Il devrait également être possible, en tout temps, de s'assurer de la qualité des informations utilisées pour prendre une décision à son sujet. En garantissant un droit d'accès et de validation des informations relatives à une transaction ou à une décision, on procure au citoyen un droit de maîtrise continu et ciblé sur ses données personnelles. Une telle exigence accroît aussi l'incitation à ne conserver

---

25 Pierre TRUCHE, Jean-Paul FAUGERE et Patrice FLICHY, *Administration électronique et protection des données personnelles livre blanc,* Rapport au ministre de la fonction publique et de la réforme de l'État, Paris, La documentation française, 2002, p.77. < http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtml >

26 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf >.

que les informations nécessaires et à mettre en place les moyens d'en assurer la qualité.

E) L'exigence de qualité

Dans un monde où l'information a vocation à circuler de plus en plus, le défi est d'assurer que l'information sera de qualité adéquate pour chacune des utilisations. La circulation des informations doit être assortie de garanties à l'égard de la qualité des informations. La qualité est une composante du lien de confiance qui doit nécessairement exister entre l'usager et l'administration. Si l'usager-citoyen n'a pas la certitude que tout est mis en œuvre afin d'assurer que les décisions sont prises avec les informations de la plus grande qualité possible, il n'aura pas confiance. C'est donc vers la recherche de l'efficacité de la régulation des données personnelles qu'il convient de mettre les efforts plutôt que de s'employer à essayer d'accroître le champ d'application des lois, même à l'égard des données publiques.

Le droit intervient pour identifier la qualité des informations à utiliser. Les personnes concernées se voient à ce titre reconnaître un droit d'accès et de rectification aux données qui les concernent. Dans l'une des rares tentatives de vérifier l'application effective de ces exigences de la Loi Informatique et Libertés, Valérie Sédallian relate qu'elle est allée de surprises en surprises devant le laxisme de plusieurs détenteurs de données personnelles quant à la sécurité des données et surtout l'exercice effectif du droit d'accès et de rectification[27].

Dans la plupart des situations, la qualité de l'information s'apprécie en fonction du contexte. Une information peut répondre convenablement à un besoin alors qu'elle sera nettement insuffisante, voire contre-indiquée, dans un autre contexte. Dans le contexte des interactions au sein des réseaux, il devient possible d'évaluer, de concert avec la personne concernée, si l'information répond aux exigences qualitatives requises pour la décision qui doit être prise. Ainsi, en renforçant les lois

---

[27] Valérie SÉDALLIAN, « La loi Informatique et Libertés vue par la « France d'en bas » ou le récit de Candide au pays des merveilles »,< http://www.juriscom.net/pro/visu.php?ID=79 >.

de protection des données de dispositions prohibant le recours à certains types d'information pour la prise de certaines décisions, on obtiendrait une diminution de la propension à recourir à des données non-pertinentes ou inexactes pour décider à l'égard des usagers des services publics ou privés.

En matière d'accès et de rectification- des droits rarement invoqués- des mises à jour sont nécessaires. Si des recours sérieux étaient mis à la disposition des citoyens et effectivement appliqués, il deviendrait possible de rendre plus risquées et non-rentables les pratiques attentatoires au droit à la vie privée. Au lieu de cela, on se complaît dans un jovialisme de bon aloi, recherchant le « règlement à l'amiable » des plaintes. Par exemple, au Québec, jamais la Commission chargée de l'application de la loi sur les données personnelles dans le secteur privé n'a jugé opportun d'intenter des poursuites pénales à l'encontre des entreprises qui font le commerce des données relatives au crédit. Pourtant, ces entreprises font l'objet de plusieurs dizaines de plaintes par année et les consommateurs qui en ont le courage doivent intenter des recours civils pour être indemnisés des dommages causés par la circulation de renseignements erronés sur leur crédit.

En somme, en prenant au sérieux les exigences de qualité des données plutôt que de s'épuiser à en empêcher la circulation, on améliorerait de beaucoup de protection de la vie privée des citoyens. Cela suppose des mécanismes de sanction conséquents.

F) Des mécanismes effectifs de sanction

Il y a des informations portant sur les personnes et qui ont de l'importance pour d'autres. Par exemple, il existe des informations à caractère public qui peuvent être consultées afin de prendre une décision éclairée Le seul fait que de telles informations présentent une possibilité d'être utilisées de manière abusive ne doit pas conduire à les censurer à titre préventif. À l'égard des possibilités d'usage abusif des informations publiques, il faut plutôt organiser des mécanismes efficaces de sanction une fois avérés les usages abusifs. Une telle approche évite de censurer les informations de manière préventive mais réserve des sanctions dissuasives pour les situations où il y a usage abusif de données. À défaut d'opter pour une telle approche, il est à craindre que l'on se retrouvera dans un

monde où il n'y aura plus d'archives, plus d'informations disponibles dès lors que celles-ci peuvent porter sur une personne.

L'efficacité de la protection de la vie privée est tributaire de l'existence de possibilités réelles d'exercice des recours lorsqu'il y a eu violation. Le principe est ainsi décrit par Yves Poullet :

> […] dans la même mesure où Internet facilite, pour les fournisseurs de services de communications électroniques, la collecte et le traitement des données, ceux-ci doivent permettre à l'utilisateur de profiter du même médium pour l'exercice plus aisé de leurs droits.[28]

Il s'agit d'utiliser les environnements électroniques pour assurer l'efficacité de l'exercice des droits des personnes. Yves Poullet explicite ainsi comment ce concept pourrait contribuer à assurer une application plus efficace du droit à la vie privée :

> […] le droit d'une personne concernée peut s'exercer plus aisément par un simple clic sur un sigle permettant l'accès direct à un 'privacy statement' […] La personne concernée peut être amenée à exercer son droit au consentement ou son droit d'opposition directement en ligne. En ce qui concerne le droit d'accès proprement dit, c'est-à-dire le droit de connaître les données enregistrées, leur origine, la logique du traitement, etc. […] on peut même imaginer qu'il s'exerce en ligne par une demande signée électroniquement. Enfin, le droit de recourir en cas de contestation relative à la pertinence ou la qualité d'une donnée […] pourquoi ne pas permettre son exercice, voire sa résolution, par des mécanismes électroniques de saisine et de règlements des conflits.[29]

La généralisation des activités dans les réseaux doit s'accompagner de la mise en place d'outils appropriés, préférablement située au sein

---

[28] Yves POULLET « Internet et vie privée : entre risques et espoirs », (2001) 120 *Journal des tribunaux* 155.

[29] Yves POULLET « Internet et vie privée : entre risques et espoirs », (2001) 120 *Journal des tribunaux* 155.

même de ces environnements afin d'assurer l'exercice efficace des droits des personnes. On voit mal comment il sera possible de maintenir un processus judiciaire ou quasi-judiciaire opérant à la vitesse de l'escargot alors que les transactions s'effectuent à la vitesse de la lumière!

Conclusion

Il a été ici question du défi d'assurer l'ajustement du cadre normatif de la protection de la vie privée afin de le rendre efficace dans les environnements de réseaux. Lucas, Devèze et Frayssinet rappelent que :

> C'est entre le discours parfois paranoïaque qui voit Big Brother partout et celui lénifiant ou intéressé qui refuse de voir les réalités et les potentialités de la technique en face, que doit se situer l'analyse raisonnée des dangers pour les droits et libertés des personnes engendrée par les nouvelles technologies de l'information et de la communication.[30]

Il faut prendre acte des mutations que la généralisation des environnements en réseaux provoque dans les conditions de production et de circulation des informations. Ces mutations appellent la mise en place d'un cadre efficace pour assurer la protection des droits des citoyens. Ce n'est pas en laissant persister un cadre juridique agissant comme un blocage qu'on assure la protection effective de la vie privée. Il faut, au contraire, recentrer le cadre juridique de l'information sur les personnes de manière à protéger effectivement la vie privée dans les contextes diversifiés des réseaux.

Les conceptions fondées sur la suprématie de la vie privée sans égard à la nécessité d'articuler ce droit avec les impératifs de l'exercice des autres droits, constituent des approches dangereuses pour le développement d'un droit des environnements de réseaux qui soit vraiment cohérent avec les principes démocratiques. Ces conceptions excluent la réflexion sur les moyens pour assurer la protection effective de la vie privée. Pourtant, il est nécessaire d'examiner sereinement les techniques permet-

---

30 André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n° 7.

tant d'assurer une protection équilibrée de la vie privée des personnes vivant en société et des autres valeurs qui contribuent, elles aussi, à assurer la dignité humaine.

La modernisation effective du droit de la protection des données personnelles passe par une relecture critique des applications qui en a été faite et une évaluation lucide des contextes dans lesquels circulent les informations. Ce serait affaiblir ce droit que de se réfugier dans une frileuse défense des façons de faire héritées des époques antérieures puisque cela accroît les risques d'une protection purement formelle, passant à côté des véritables périls.

La généralisation des environnements de réseaux ne laisse guère le choix : il devient de plus en plus urgent d'ajuster un régime de protection de la vie des personnes qui reflète toute la complexité du cyberespace. La démarche doit être menée en reconnaissant le fait que l'information sur les personnes n'a jamais été et ne peut être détachée de l'environnement global dans lequel évoluent les personnes. C'est de cette façon qu'il faut envisager la modernisation du régime de protection de la vie privée pour le monde en réseaux.