



**GRUPE "INFORMATIQUE & LIBERTES 2.0 ?"**

## **LE NOUVEAU PAYSAGE DES DONNEES PERSONNELLES : QUELLES CONSEQUENCES SUR LES DROITS DES INDIVIDUS ?**

NOTE DE TRAVAIL A COMMENTER – JANVIER 2009

### **Membres du groupe de travail :**

- Arnaud Belleil
- Yves Deswarte
- Renaud Francou
- Daniel Kaplan
- Emmanuel Kessous
- Olivier Iteanu
- Jean-Marc Manach
- Thierry Marcou
- Charles Nepote
- Sylvie Rozenfeld
- Jean-Baptiste Soufron
- Vincent Toubiana

---

<b>A propos de ce document : pourquoi, pour quoi faire, comment contribuer ? .....</b>	<b>2</b>
<b>Introduction : "Informatique et libertés 2.0" ?.....</b>	<b>3</b>
<b>Première partie : Le nouveau paysage des données personnelles .....</b>	<b>4</b>
Partout, tout le temps, de toutes parts : le nouveau régime des "données à caractère personnel" .....	5
De nouveaux moteurs comportementaux et économiques .....	7
Le nouveau contexte de l'action publique .....	10
<b>Seconde partie : De la protection à la maîtrise : nouveaux droits, nouveaux outils .....</b>	<b>12</b>
De nouvelles marges de manœuvre pour les individus .....	13
De nouvelles réponses collectives .....	15
Retracer des "lignes rouges" .....	17
<b>Conclusion provisoire .....</b>	<b>18</b>

## **A PROPOS DE CE DOCUMENT : POURQUOI, POUR QUOI FAIRE, COMMENT CONTRIBUER ?**

Le travail "Informatique & Libertés 2.0 ?" (notez le point d'interrogation) est né au sein du programme "Identités actives" de la Fing. Ce programme s'intéresse aux manières dont les individus, se servent de leur(s) identité(s) numérique(s) pour devenir stratèges de leur propre existence.

De manière transverse aux différents thèmes abordés par le programme, nous avons pressenti que l'émergence de ces pratiques, au travers par exemple des sites sociaux, des blogs ou encore des pseudonymes et avatars qui fleurissent sur les réseaux, questionnait aussi l'édifice juridique actuel autour de la protection de la vie privée.

Un groupe de travail s'est réuni pour approfondir cette intuition. La note de travail qui vous est soumise rend compte de ses travaux.

Nous en sommes à la fois satisfaits et insatisfaits.

Nous pensons qu'elle souligne quelques transformations importantes qui doivent être prises en compte à un niveau politique autant qu'économique ou technique. Nous avons le sentiment de proposer quelques pistes nouvelles.

Mais il reste du travail pour en faire une plate-forme partagée à partir de laquelle des recommandations peuvent émerger, des projets peuvent naître. Pour certains lecteurs, le document devrait s'intéresser plus précisément aux risques autant qu'aux opportunités. Pour d'autres, il ne fait pas assez le tri entre de vraies nouveautés et des tendances bien connues et traitées depuis longtemps par les acteurs du monde "informatique & libertés". Enfin, les pistes de réponse demeurent sommaires et certainement incomplètes.

Nous avons donc choisi de mettre le document de travail en ligne, en l'état, pour le soumettre à discussion.

Vous pouvez le lire sur le web ou le télécharger. Vous pouvez publier vos commentaires ou nous les envoyer par retour de mël à [charles.nepote@fing.org](mailto:charles.nepote@fing.org), [rfrancou@fing.org](mailto:rfrancou@fing.org) et [dkaplan@fing.org](mailto:dkaplan@fing.org).

Ces commentaires peuvent proposer des corrections, des rectifications, des idées nouvelles, ou faire état de projets ou de réalisations qui vous paraîtraient pertinents.

A partir de vos contributions, nous produirons une ou plusieurs autre(s) version(s) de ce document, dans l'objectif d'une publication au plus tard mi-2009. Avant d'y parvenir, nous vous proposerons plusieurs manières d'interagir, en ligne et hors ligne. Même après publication, le contenu du document restera librement accessible et utilisable, et soumis à discussion. Les contributeurs seront enfin tous cités dans la publication, à supposer bien sûr qu'ils l'acceptent.

Nous vous remercions par avance de votre contribution à ce travail collectif.

## **INTRODUCTION : "INFORMATIQUE ET LIBERTES 2.0" ?**

Les 30 ans de la loi Informatique & Libertés offrent l'occasion de réfléchir à l'avenir de la vie privée dans nos sociétés numérisées, en tenant compte des évolutions intervenues depuis dans les pratiques sociales, l'économie, les politiques publiques, la technologie et son emploi.

Certains des défis auxquels la loi de 1978 fait face sont déjà amplement documentés : le passage d'une informatique lourde et centralisée à une informatique en réseau et décentralisée ; une loi conçue pour faire face à des menaces venant des acteurs publics dans un monde où la grande majorité des fichiers sont privés ; une loi nationale face à des acteurs mondiaux et des réseaux sans vraie frontière, etc.

Mais d'autres nous paraissent de nature à déplacer le terrain même sur lequel s'est constitué l'édifice juridique actuel en matière d'informatique et de libertés – qui ne se limite d'ailleurs pas à la loi du même nom. Le droit d'expression, le droit de propriété, le droit à l'image, sont également concernés.

### **Du village fortifié à la tête de pont**

Il ne s'agit pas non plus d'envisager le (ou les) droit(s) sous un angle uniquement protecteur. Les individus ne se préoccupent pas seulement (quand ils s'en préoccupent) de défendre leur vie privée, il est tout aussi important pour eux de constituer, d'affirmer, d'exploiter leur identité publique dans un monde en réseau.

Autrement dit, nous devons passer d'une approche de la vie privée et de l'identité publique perçues comme une sorte de village fortifié – entouré de prédateurs, bien protégé, mais qui n'envisage pas de déborder de ses propres frontières – à la tête de pont, que l'on défend certes, mais qui sert d'abord à se projeter vers l'avant.

### **Des pistes à discuter**

Dans le cadre du programme "Identités actives" de la Fing, un groupe de travail pluridisciplinaire et resserré s'est fixé pour but d'explorer, parmi les nouveaux défis auxquels la démarche "informatique et libertés" fait face aujourd'hui et pour l'avenir, ceux qui peuvent être considérés comme de "nouveaux paradigmes". Par "nouveaux paradigmes", nous entendons des transformations profondes du contexte même dans lequel les questions se posent et les réponses se proposent.

Cette note propose une première synthèse, intermédiaire, des réflexions et des propositions de ce groupe.

Elle doit être considérée comme une plate-forme de discussion, plutôt que comme une production finie. Les pistes qu'elle esquisse doivent être affinées, critiquées, retravaillées. Nous assumons ces limites. Notre espoir est que cette note contribue à ouvrir le débat, à l'orienter sur des voies nouvelles qui nous paraissent encore peu explorées.

## **PREMIERE PARTIE : LE NOUVEAU PAYSAGE DES DONNEES PERSONNELLES**

*Nous avons l'habitude d'aborder le lien entre informatique et vie privée sous l'angle de la protection des individus face à des entreprises ou un Etat avides de données, dans un contexte où les "fichiers" sont des bases de données structurées, issues de formulaires.*

*Tout cela change profondément.*

*D'une part, toute information, toute image, toute contribution en ligne, peut acquérir un jour un caractère personnel et circuler, se répliquer au point de devenir difficilement effaçable. D'autre part, les individus se préoccupent au moins autant de s'exposer, de valoriser leur image, d'étendre leur réseau de relations, que de se protéger. Enfin, tant en ce qui concerne les entreprises que l'Etat, les informations personnelles constituent la matière première essentielle d'une "économie de la connaissance" qui s'appuie sur la personnalisation, la réactivité, l'agrégation de services autour de l'individu, la mobilité et la continuité.*

## PARTOUT, TOUT LE TEMPS, DE TOUTES PARTS : LE NOUVEAU REGIME DES "DONNEES A CARACTERE PERSONNEL"

Le changement d'échelle, en termes de nombre de fichiers, d'acteurs ainsi que de sources de collecte, capture et traitement d'informations à caractère personnel, constitue la première évolution majeure du contexte.

Ce sujet paraît *a priori* bien connu, mais en réalité, plusieurs phénomènes récents demeurent assez mal pris en compte.

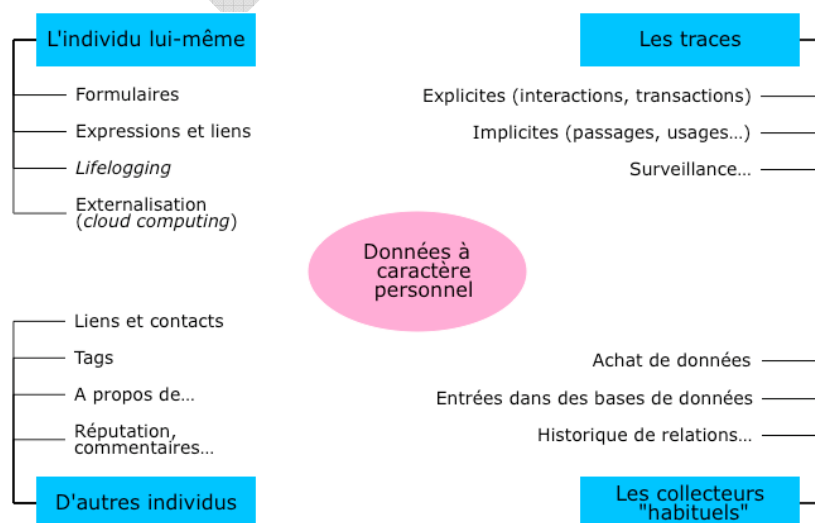
### Des données structurées aux grains d'information

Au-delà des données classiquement répertoriées dans les champs de bases de données, et dont la signification est en général assez explicité, on assiste à la multiplication de données à caractère personnel d'une nature beaucoup plus informelle : productions et expressions diverses d'un individu, messages, contacts, relations et liens, jugements de ou à propos de la personne, commentaires, images, rumeurs, traces de passage ou d'usage... autant de "grains" d'information, jusqu'ici difficilement exploitables à grande échelle, mais dont la forme numérique permet désormais de faire plus aisément usage.

Ces informations peuvent avoir été fournies par l'individu concerné, ou par des tiers. Elles sont souvent informes, incluses de fait et sans indication particulière dans un texte ou une image. Mais elles deviennent de plus en plus aisément exploitables grâce aux moteurs de recherche, aux systèmes de *datamining* ou d'analyse sémantique, aux logiciels de reconnaissance des formes, aux graphes de réseaux sociaux, etc.

### Une multitude de sources nouvelles

Les sources de données à caractère personnel susceptibles d'être exploitées se multiplient, tant en nombre (ce qui ne constituerait pas nécessairement une évolution majeure) que dans leurs natures.



Au-delà des sources classiques, entreprises et administrations, on constate que :

- Les individus eux-mêmes transmettent, publient, externalisent... des volumes croissants d'information qui peuvent avoir un caractère personnel, voire intime.
- Des tiers peuvent également produire des informations concernant un individu : en parlant de lui sur un blog, en étiquetant une photo de lui, en commentant une de ses productions, en se liant à lui, en évaluant sa qualité de rédacteur sur un site collaboratif ou de vendeur sur un site d'enchères...
- Les machines captent, produisent, stockent et analysent des myriades de traces, certaines d'une manière assez explicite quand il s'agit de mémoriser une interaction avec l'individu, d'autres moins, voire à l'insu de l'individu (cas de la vidéosurveillance avec reconnaissance de visage ou de plaque minéralogique).

La démocratisation des moyens de "surveillance" est un fait acquis et intégré. Ainsi, de très nombreuses personnes "googlent" les individus qu'elles connaissent ou rencontrent, ou avec lesquels elles ont rendez-vous, ou qu'elles envisagent de recruter.

### **Des données personnelles "par destination"**

Les deux points qui précèdent ont une conséquence commune : beaucoup d'informations ne sont pas *a priori* des "informations personnelles", construites et collectées comme telles, mais elles peuvent acquérir un caractère personnel *a posteriori* : par analyse, recoupement, traitement sémantique, commentaire d'un tiers, etc. Et les dispositifs susceptibles d'effectuer cette transformation, intentionnellement ou non, se multiplient.

### **L'effacement, cible mouvante**

Enfin, il devient extrêmement difficile d'effacer de manière sûre une donnée une fois que celle-ci a commencé sa vie dans les systèmes et les réseaux :

- Parce que beaucoup de données susceptibles d'avoir un caractère personnel ne sont pas nécessairement considérées comme telles *a priori*, mais seulement au hasard (plus ou moins provoqué) de divers recoupements ;
- Parce que les informations se répliquent très rapidement dans une multitude de copies, caches, sauvegardes, republications, etc., le plus souvent sans le moindre contrôle de la part du premier site d'enregistrement ;
- Parce que les entités juridiques qui enregistrent les informations originelles sous-traitent souvent le stockage physique à d'autres, etc.

### **En conséquence, il devient de plus en plus difficile :**

- De savoir *a priori* si une information est ou pourrait avoir un "caractère personnel" ;
- De savoir quand, comment, auprès de qui faire jouer un éventuel droit d'accès ;
- De s'assurer qu'une information est bien corrigée, ou oubliée, même si l'on en a obtenu le rectification ou l'effacement dans certaines bases.

## DE NOUVEAUX MOTEURS COMPORTEMENTAUX ET ECONOMIQUES

---

L'édifice "informatique et libertés" considère que les individus sont en situation défensive face à des organisations qui cherchent à collecter des informations dans un but, soit de contrôle, soit de vente, soit de recrutement. Or les pratiques des uns comme des autres, et les motivations associées, ressemblent de moins en moins à cette description.

### La puissance de la commodité

Le premier constat, suffisamment documenté pour avoir reçu le nom de *privacy paradox* ("paradoxe de la vie privée") est que les individus expriment régulièrement leur inquiétude d'être "fichés", tout en donnant d'une manière très libérale des informations de tous ordres quand on les leur demande.

Ce paradoxe ne s'explique pas par un manque d'information de la part des consommateurs. Les études menées par Caroline Miltgen<sup>1</sup>, par exemple, montrent que les individus arbitrent en fonction d'une véritable analyse de risque – mais que les bénéfices attendus de la fourniture d'information, en termes de commodité notamment (obtenir plus aisément un service, bénéficier d'avantages, être reconnu la prochaine fois...) l'emportent généralement sur les craintes.

### L'exposition volontaire

Le second constat est moins habituel : les individus, en ligne, exposent délibérément un très grand nombre d'informations sur eux-mêmes, afin de se forger une identité sociale, de se montrer aux autres, d'enrichir leur réseau de relation, etc. :

- Publication (blogs, photos, vidéos...) : s'exprimer, s'exposer, gérer son image...
- Socialisation (réseaux sociaux) : se présenter pour élargir et entretenir son réseau, se présenter au travers de son réseau ("dis-moi qui tu connais, je te dirai qui tu es")
- Réputation : visibilité, échanges de liens, notation, réputation de vendeur ou d'acheteur... exposer et influencer le jugement que les autres portent sur soi

Ainsi, bien loin de songer à se protéger, un très grand nombre d'individus sont au contraire engagés dans de véritables stratégies de visibilité. Leur objectif devient de maîtriser leur image, et non de la dissimuler.

### Les données "sensibles" en tension

Pour entrer en relation avec d'autres, les données considérées comme "sensibles" par la loi, parce qu'elles peuvent donner lieu à des discriminations, sont souvent, précisément, les plus pertinentes : l'orientation sexuelle, les opinions politiques et religieuses, l'origine ou le sentiment d'appartenance ethnique ou communautaire...

---

<sup>1</sup> Caroline Miltgen, "L'internaute et ses données : ce qu'on dit, ce qu'on fait", Internet Actu, 2006 : [www.internetactu.net/2006/02/08/linternaute](http://www.internetactu.net/2006/02/08/linternaute) - et sa thèse ultérieure.

Le formulaire de "profil" de Facebook demande ainsi, dès la première page, quelles sont nos orientations politiques et religieuses. Il s'enquiert du statut amoureux et, si l'utilisateur cherche un partenaire, du sexe de l'âme sœur recherchée. Tout ceci apparaît ensuite dans le profil public. De telles questions, surtout les premières, sont probablement contraires à la loi française, mais si Facebook ne les posait pas, sa valeur en tant que site de réseautage en serait nettement réduite. On notera toutefois que les sites de réseautage à vocation purement professionnelle, tels l'Américain LinkedIn ou le Français Viadeo, ne posent pas de telles questions.

### **Les données personnelles, matière première de l'économie numérique**

Les services de l'économie numérique sont personnalisés, contextualisés, fédératifs, relationnels. Les données personnelles en constituent une matière première essentielle. Comme le relève un récent rapport du *think tank* britannique Demos<sup>2</sup>, on ne peut guère dissocier les avantages de l'économie numérique de l'usage croissant des données à caractère personnel.

- Les consommateurs s'attendent à ce que les entreprises les reconnaissent et adaptent leurs propositions à leur situation et leurs besoins (voire au contexte du moment : le moment, le lieu, le canal, etc.), ainsi qu'à l'historique de leur relation ;
- Les services se structurent souvent par agrégation de "briques" produites par plusieurs acteurs. La pertinence de cette agrégation dépend avant tout de la compréhension de qui est l'utilisateur et dans quel contexte il se situe ;
- De nombreux services fondent leur proposition de valeur sur la qualité du *matching*, de la mise en relation qu'ils proposent entre offre et demande, personnes, informations, goûts – ce qui suppose une connaissance fine de chaque individu ;
- Enfin, les entreprises personnalisent leurs offres – et plus encore, leurs prix – à partir de modèles d'optimisation de plus en plus élaborés. C'est ainsi qu'elles parviennent à fidéliser leurs clients tout en attirant de nouveaux, à minimiser leurs stocks et maximiser leurs taux d'occupation, à réagir plus vite aux évolutions du marché.

### **L'attention, nouveau bien rare**

La fameuse phrase sur le "temps de cerveau disponible" résume bien la situation de l'économie contemporaine de l'information : l'information, les contenus, les messages surabondent, et le bien rare devient l'attention du consommateur.

Capter et exploiter les "marques d'attention" du consommateur (ses traces, notamment) est l'une des seules manières durables de générer des revenus pour les médias, les supports numériques, mais aussi les contenus et services en ligne. Ceci explique l'importance prise par les acteurs qui parviennent à occuper une place centrale, au carrefour des échanges entre les utilisateurs et les services (moteurs de recherche par exemple) ou entre les utilisateurs eux-mêmes (réseaux sociaux, webmails...).

**En se focalisant sur la seule *protection* des informations à caractère personnel, on ne rend pas compte du caractère central** de la dissémination, la captation,

---

<sup>2</sup> "FYI – The new politics of personal information", 2007 : [www.demos.co.uk/publications/fyi](http://www.demos.co.uk/publications/fyi)

l'exploitation et l'échange de ces informations dans notre société et notre économie numériques.

En revanche, comme le relève Demos, *"le champ de bataille de l'information personnelle est désormais le lieu où les distinctions rationnelles entre différentes catégories de personnes, fondées sur leurs données, produit des différences dans ce qu'ils vivent et ce à quoi ils ont accès."* Autrement dit, le problème réside plutôt dans l'influence que les individus peuvent, ou non, avoir sur les décisions qui sont prises à partir de l'information qu'on possède sur eux : ce à quoi ils ont droit ou non, ce qu'on leur propose ou non, quels tarifs leur sont appliqués, etc.

DRAFT

## **LE NOUVEAU CONTEXTE DE L'ACTION PUBLIQUE**

---

Du côté des acteurs publics, le contexte a également changé depuis 1978. L'équilibre complexe entre l'Etat protecteur des individus, l'Etat défenseur de l'ordre public et l'Etat fournisseur de services, s'est nettement déplacé en faveur des deux dernières missions.

### **L'Etat défenseur de l'ordre public : une tendance sécuritaire accentuée, et dans une large mesure consentie**

Issue des attentats du 11 septembre 2001, ou bien facilitée par l'émotion qu'ils ont provoquée, une vague sécuritaire a recouvert la plupart des pays développés. Ce sujet a été amplement évoqué par ailleurs.

Cette tendance suscite des réactions, mais elle est globalement tolérée par la société civile, dont la tolérance face aux risques de tous ordres est également devenue plus faible. Des initiatives qui n'auraient vraisemblablement pas été admises auparavant voient aujourd'hui le jour :

- Pour protéger les personnes vulnérables, par exemple en équipant de bracelets électroniques des malades d'Alzheimer ;
- Pour protéger la société contre des personnes dangereuses (délinquants sexuels libérés) ou considérées comme potentiellement dangereuses (le fichier ADN sans cesse étendu à de nouvelles personnes, le projet de dépistage précoce des prédispositions asociales chez les enfants) ;
- Pour surveiller par défaut les lieux publics (explosion de la vidéosurveillance)...

Ces tendances sont renforcées par l'amélioration et la maturation des technologies sécuritaires : biométrie, identification sans contact (Rfid notamment), reconnaissance de formes (associée par exemple à la vidéosurveillance), datamining... La tentation d'en exploiter toutes les possibilités est difficilement résistible.

### **L'Etat fournisseur de services : une recherche d'amélioration et de personnalisation des services publics**

Dans le but de mieux servir les usagers et/ou de gagner en productivité, les administrations font de plus en plus usage des méthodes issues du privé. Le pré-remplissage des feuilles d'impôt, ou le changement d'adresse en "un clic", relèvent de cette démarche et simplifient clairement la vie des usagers. Ils nécessitent cependant une exploitation, un partage et un stockage d'informations personnelles qui vont plus loin qu'auparavant.

Pour gagner en productivité, en souplesse et en réactivité, ou tout simplement pour réduire ses budgets, les acteurs publics sont par ailleurs amenés à collaborer étroitement avec des entreprises, parfois en sous-traitance, parfois en partenariat :

- Comme les autres entreprises, les services de l'Etat sous-traitent un nombre croissant d'activités informatiques, mais aussi de relation avec les usagers (centres d'appels, etc.) auprès d'entreprises spécialisées. Dans d'autres cas, des entreprises privées gèrent intégralement un service public (transports, prisons...). Ceci n'est pas critiquable en soi, mais il est néanmoins clair que des quantités massives de données relatives aux usagers circulent hors des murs de l'administration ;

- Des personnels assermentés, tels que les postiers, sont également chargés de collecter des informations afin de renseigner des bases de données de géomarketing, qui seront ensuite exploitées et commercialisées auprès d'entreprises ;
- Des dispositifs d'identification issus du secteur public sont de plus en plus exploités à d'autres fins. C'est le cas du passe Navigo, créé pour les transports en Ile de France, utilisé aujourd'hui pour Velib' et demain pour d'autres services urbains. L'Etat envisage également de profiter de la sécurité qu'offre la future Carte d'identité électronique pour en faire le support d'authentification de transactions privées.

En tant que fournisseur de services, l'Etat partage désormais, dans une large mesure, les préoccupations, les pratiques, les outils et les indicateurs du secteur privé. Comme pour les entreprises, les données à caractère personnel sont pour lui la matière première à partir de laquelle il étend et personnalise ses services, il réduit ses coûts, il mesure sa performance.

### **L'Etat garant des libertés individuelles : une baisse du niveau de contrôle sur les propres actions de l'Etat**

La révision de la loi de 1978 intervenue en 2004 a significativement réduit le niveau de contrôle de la Cnil sur les activités de l'administration, comme l'illustre l'épisode récent du passeport biométrique. Ce point a également fait l'objet d'une abondante littérature.

L'avocat Alain Bensoussan parle aujourd'hui d'un "sur-encadrement de l'activité des entreprises" et d'un "sous-encadrement de l'activité de l'Etat". Il s'agit là d'un retournement par rapport à la situation de 1978, la loi "Informatique et libertés" ayant été votée en réaction à un vaste projet d'interconnexion des fichiers de l'Etat et de la Sécurité sociale, nommé SAFARI. Il est vrai que depuis, la plupart des regroupements du projet SAFARI ont été effectués, les uns après les autres, dans des situations certes mieux définies.

**Nous ne faisons pas face à une dérive dictatoriale.** La plupart des évolutions décrites ici sont pour l'instant bien acceptées, ou du moins ne suscitent-elles guère d'opposition au-delà d'un petit cercle de spécialistes et de militants. Dans de nombreux cas, elles contribuent réellement à améliorer la qualité du service rendu aux usagers.

Le niveau global de vigilance vis-à-vis des actions de l'Etat connaît une baisse sensible : bien des projets contre lesquels la loi de 1978 avait été conçue ont été réalisés, et au-delà. La loi est la même, ou presque, mais les limites de l'acceptable ont clairement reculé.

L'absence de réaction des citoyens ne traduit pas non plus une grande confiance. Sondage après sondage, les Français se disent gênés par le fait que de nombreuses informations les concernant soient stockées dans des fichiers et s'estiment insuffisamment informés sur leurs droits. L'Etat suscite aujourd'hui moins de méfiance que les entreprises, mais plus ses pratiques se rapprocheront de celles des entreprises, et plus les fonctions d'ordre public et de service se mêleront (à des fins, par exemple, de contrôle fiscal), plus son image se banalisera. Alors que la désaffection des citoyens vis-à-vis de la vie démocratique préoccupe tous les élus, il est temps d'y réfléchir.

## **SECONDE PARTIE : DE LA PROTECTION A LA MAITRISE : NOUVEAUX DROITS, NOUVEAUX OUTILS**

*Le contexte d'application des principes relatifs à la protection des libertés et de la vie privée dans la société numérisée a donc profondément changé. Des problèmes nouveaux sont apparus ; d'autres ont changé d'échelle à un point tel qu'on ne peut plus du tout les aborder comme auparavant.*

*Cela ne signifie pas que l'édifice conçu en 1978 et réformé en 2004<sup>3</sup> soit devenu obsolète. Certains droits, certaines protections doivent être réaffirmés et appliqués. Des "lignes rouges" doivent être redessinées.*

*Mais il faut aussi repenser les manières d'atteindre ces objectifs. Il faut passer d'une protection passive qui serait garantie à l'individu de l'extérieur, à une forme de maîtrise qui tient compte des arbitrages, des choix, des désirs et des capacités de chacun. Il faut passer des protections fixes aux défenses mobiles, du village fortifié à la tête de pont. Sinon, les objectifs que vise l'édifice "Informatique et libertés" deviendront impossibles à atteindre et certains des droits, purement formels.*

*Nous proposons ici une première réflexion sur ces nouveaux droits et ces nouveaux outils – les deux étant indissolublement liés. Nous focaliserons notre attention, d'abord sur les individus, ensuite sur les acteurs et les réponses collectives.*

*Ces propositions doivent être reçues comme un appel au débat, et non comme un produit fini, ni une plate-forme programmatique.*

---

<sup>3</sup> En transposition, fort tardive, d'une directive européenne de 1995.

## DE NOUVELLES MARGES DE MANŒUVRE POUR LES INDIVIDUS

---

Les protections érigées par les lois actuelles s'assimilent pour la plupart à des défenses "fixes" : elles définissent ce que les entreprises ou les administrations n'ont pas le droit de faire. Dans un monde en réseau, leur efficacité ne peut que décroître. Une première évolution pourrait donc consister à concevoir des défenses "mobiles", destinées à redonner aux individus des marges de manœuvre alors même que des informations personnelles de toutes natures sont collectées, exploitées et échangées.

### Des défenses fixes aux défenses mobiles

Le droit d'accès et de rectification entre dans cette catégorie, mais il est peu utilisé et peu efficace lorsqu'on ignore ce qui est collecté par qui, lorsque les données sont répliquées en de multiples endroits ou encore, lorsque des informations acquièrent *a posteriori* un caractère personnel.

D'autres droits pourraient alors être explorés :

- Un **droit à l'anonymat**, qui pourrait par exemple exiger un niveau de service minimal sans identification. Ce droit concernerait au premier chef les individus, mais il aurait aussi des conséquences pour les organisations, telles que l'obligation (déjà présente dans certains cas) d'anonymiser des données après quelque temps, ou bien avant de les croiser en vue de traitement statistiques.  
Du côté des individus, il existe aussi des moyens de rendre anonyme la navigation sur l'internet. Si certains projets privés ou militants sont connus depuis longtemps<sup>4</sup>, des entités publiques s'y engagent également : l'autorité indépendante de protection des données du Land allemand du Schleswig-Holstein soutient ainsi le projet JAP [<http://anon.inf.tu-dresden.de/>], qui fait transiter les connexions de ses utilisateurs par plusieurs serveurs intermédiaires qui les "mangent" de telle manière que personne, pas même ces intermédiaires, ne puisse retracer qui s'est connecté à quoi.
- Un **droit au "mensonge légitime"**, dès lors qu'on estime excessif que ce qui est demandé pour accéder à un service, mais que l'on souhaite quand même y accéder ;
- Un **droit à l'"hétéronymat"**, autrement dit à la construction de pseudonymes "riches", à de véritables personnalités alternatives séparées de manière étanche de la personnalité civile qui les exploite – sur le modèle, non pas des "pseudos" utilisés sur les forums en ligne, mais des identités alternatives que choisissent certains écrivains pour explorer d'autres genres ou d'autres styles<sup>5</sup> ;
- Un **droit à récupérer ses données**, c'est à dire à obtenir sous une forme exploitable tout ce qu'un acteur détient sur la personne.  
Une première étape pourrait consister à exiger que l'exercice du droit d'accès et de rectification puisse se faire sous forme électronique, dans des délais resserrés, voire en temps réel. Mais ce droit a une vocation plus large. Il s'agit de permettre à l'individu d'exploiter lui-même, à ses propres fins, les données qu'il a confiées à d'autres. La

---

<sup>4</sup> Liste non exhaustive : [www.livinginternet.com/i/is\\_anon\\_sites.htm](http://www.livinginternet.com/i/is_anon_sites.htm)

<sup>5</sup> Pour une définition de l'"hétéronymat" : [www.identitesactives.net/?q=lexique-terme10-heteronyme](http://www.identitesactives.net/?q=lexique-terme10-heteronyme)

"portabilité" des profils ou des listes de contacts entre les sites de réseaux sociaux sur l'internet, soit pour migrer de l'un à l'autre, soit pour les rendre plus ou moins interopérables, en serait par exemple une application.

- Enfin, un **droit opposable de recours** face aux décisions prises par une entreprise ou une administration à partir du profil d'un individu : dans quel segment il se trouve classé, quels tarifs lui sont appliqués, quels droits lui sont reconnus ou déniés, quelles offres lui sont proposées ou masquées...

Ces différents droits convergent peut-être vers une sorte de droit patrimonial, de propriété et de valorisation de ses données personnelles et de son image. Il appartient cependant à des juristes d'en tirer ou non de telles conséquences.

### **Des outils, eux-mêmes protégés, pour négocier ses données**

Ces "défenses mobiles" ne peuvent attendre le passage devant un tribunal ou une autorité quelconque pour s'appliquer. La première étape consiste à les traduire dans des outils mis entre les mains des utilisateurs.

Les "**technologies de protection de la vie privée**" (PETs, pour *privacy-enhancing technologies*) regroupent un très grand nombre d'outils, mais ceux-ci demeurent complexes, peu standardisés et au final, très peu utilisés. Pour qu'ils le deviennent, il leur faut répondre aux attentes de commodité qu'expriment les utilisateurs, se standardiser et se répandre très largement.

Quelques exemples permettent d'illustrer les possibilités de ces outils :

- **Des systèmes d'"i-carte"** visent à permettre à l'utilisateur de stocker chez lui (ou chez des tiers de confiance) toutes ses données, et à organiser un dialogue explicite, homogène et intelligible, entre l'individu et l'organisation qui lui demande des informations. CardSpace de Microsoft, ou le projet Higgins piloté par IBM, sont deux représentants de ce type de système ;
- Des dispositifs permettent de "**griller**" les puces Rfid insérées dans des produits ou des emballages. Ils peuvent être possédés par des individus (ce qui est rarement le cas) ou mis en œuvre par des entreprises : GS1, l'association qui gère les standards de communication entre industrie et commerce, a ainsi recommandé aux distributeurs français de désactiver les puces Rfid lors du passage en caisse ;
- Il est possible de créer des **cartes électroniques sécurisées et anonymes** qui permettent de prouver une caractéristique (par exemple la nationalité, ou le droit de conduire) sans avoir besoin d'indiquer l'identité de leur porteur ;
- **L'"obfuscation"** (ou "assombrissement") consiste à occulter délibérément le sens d'une information et, par extension, à noyer l'information pertinente dans un "bruit" sans signification. Ainsi, TrackMeNot ou Squiggle SR, des extensions du navigateur Firefox, multiplient les requêtes aléatoires aux moteurs de recherche afin que les vraies requêtes de l'utilisateur ne renseignent en rien sur ses centres d'intérêt.

Un effort public de R&D, d'expérimentation et de déploiement pourrait soutenir le développement, la standardisation (internationale) et la diffusion de ces outils.

Enfin, il pourrait être envisagé de **protéger ces outils** en interdisant aux entreprises de les court-circuiter ou de les désactiver, un peu sur le modèle de la protection des "mesures techniques de protection" des œuvres, prévue par les directives européennes sur les droits d'auteur dans la société de l'information...

## DE NOUVELLES REPONSES COLLECTIVES

---

Les outils de protection de la vie privée sont une condition nécessaire, mais non suffisante, pour retrouver une maîtrise sur la circulation et l'exploitation des données des individus. Ils présentent l'inconvénient de faire reposer cette maîtrise sur l'individu, dont la relation avec les entreprises et les institutions est pour le moins inégale.

D'autres dispositifs doivent donc "collectiviser" le contrôle. Certains sont d'ordre politique et juridique, tandis que d'autres visent plus à organiser une pression citoyenne et économique sur les acteurs, afin de favoriser des comportements vertueux.

### Surveiller les surveillants

La première piste consisterait à exiger de ceux qui obtiennent des informations des individus, de donner en retour des informations sur eux-mêmes et sur leurs pratiques – et le cas échéant, de favoriser l'échange d'informations entre les individus au sujet de ces organisations. Une sorte de donnant-donnant, régulé par les autorités publiques et/ou par l'intelligence collective des citoyens-consommateurs.

- Il s'agirait d'abord **organiser la transparence des classements et des décisions individuelles fondés sur l'usage des données personnelles** : comment et pourquoi on classe tel individu dans quel segment, on lui applique tel tarif ou telle décision, on lui propose telle offre plutôt qu'une autre, il accède ou non à tel droit... Cette piste présente l'inconvénient majeur, du point de vue des entreprises, que le fonctionnement même d'un système de discrimination tarifaire ou de personnalisation poussée repose souvent sur son opacité : si les clients savaient comment marche le système, ils pourraient tricher avec lui, ce qui irait à l'encontre de l'optimisation recherchée. Une solution pourrait consister à réserver la connaissance du mécanisme lui-même à une autorité tenue à des règles strictes de confidentialité.
- L'autre transparence obligatoire pourrait consister à dévoiler à quelles autres entités les données concernant un individu ont été **transmises, louées, vendues**...
- Les acteurs pourraient, comme c'est déjà le cas *de facto* aux Etats-Unis, avoir l'obligation **d'informer le public si la confidentialité de leurs données a été compromise** par une erreur ou un acte de piratage ;
- Les pouvoirs publics et/ou les associations de consommateurs pourraient créer des **sites web d'échange et de remonter d'information sur les problèmes rencontrés** par les individus et sur les pratiques douteuses des entreprises : "NoteTonMarchand", "NoteTonGuichet"...
- Enfin, le dispositif attendu des **"class actions"** devrait être étendu à l'usage abusif de données à caractère personnel.

### Focaliser l'action sur les grands intermédiaires

Certains grands acteurs de l'internet jouent, de par leur position, un rôle central dans la collecte et l'exploitation des données personnelles. Ils forment une sorte d'infrastructure critique de l'économie numérique et de ce fait, ils ont sans doute vocation à être régulés comme tels.

- **Les grands moteurs de recherche** peuvent et doivent se faire imposer des règles strictes en matière de traçage, d'effacement, d'exploitation des données que leurs utilisateurs leur fournissent ou déposent chez eux. Des négociations en ce sens sont déjà en cours. Même si le contexte européen est heureusement différent, l'exemple de ce que le gouvernement chinois a obtenu de Google et de Yahoo! démontre que ces acteurs ne sont pas inaccessibles aux volontés publiques.  
On peut aussi imaginer, en suivant le chercheur Emmanuel Kessous<sup>6</sup>, que les moteurs mettent à disposition des utilisateurs des outils qui leur permettraient, même d'une manière imparfaite, de "nettoyer leur passé" en coupant certains liens issus du référencement, rendant ainsi plus difficile (mais pas impossible, car les contenus originels demeurent) la reconstitution d'un profil complet.
- **Les réseaux sociaux** et au-delà, d'autres acteurs qui jouent un rôle clé dans la mise en relation des individus, pourraient se voir imposer la **portabilité des identités**, des profils et des carnets d'adresse. Aujourd'hui, un client de Facebook qui choisirait de migrer sur une plate-forme concurrente perdrait tout l'investissement qu'il y a consenti. De même, un utilisateur de MSN Messenger ne peut pas basculer sur une autre messagerie instantanée sans perdre sa liste d'amis. Les pouvoirs publics ont su imposer la portabilité des numéros de téléphone mobile, ces cas sont du même ordre.

### Personnaliser sans identifier

Il est communément admis que pour personnaliser un service, il faut connaître l'utilisateur. Certes, mais cela ne nécessite pas toujours – et même, sans doute, pas si souvent que ça – de savoir comment il s'appelle. Le garçon de café qui reconnaît ses habitués leur servira leur boisson favorite sans connaître leur nom, ni bien d'autres choses qui les concernent. Peut-on proposer aux entreprises et aux administrations des formes de personnalisation efficaces et productives (qui répondent donc à leurs besoins économiques) qui n'exigent pas d'identification ?

C'est l'objet d'un autre groupe de travail du programme "identités actives" de la Fing. Plusieurs pistes peuvent d'ores et déjà être évoquées :

- Différentes formes de "**filtrage**" **historique et "collaboratif"**, qui consistent à déduire les attentes d'un consommateur de ses comportements passés et de leur comparaison avec les comportements d'autres utilisateurs, n'ont pas nécessairement besoin d'identification. L'usage des "cookies", petits fichiers qui permettent à des sites de "tracer" leurs utilisateurs sans nécessairement savoir qui ils sont, fournit une bonne base à ces pratiques. Des cartes de fidélisation "blanches", qui savent ce qu'a acheté un client mais ne connaissent pas son identité, font également partie des pistes réalistes.
- La **personnalisation sur le poste client** ("*client-side personalization*"), qui se fonde sur les données d'un utilisateur, sans pour autant capturer ces données : seul le résultat (une proposition personnalisée, par exemple) est connu de l'entreprise.
- Le recours à des **pseudonymes "riches"** (ou "hétéronymes"), de véritables personnalités numériques qui exprimeront les aspirations de ceux qui les portent (et donc devenir les sujets d'un dialogue commercial), sans nécessairement se recouper avec une identité civile...

---

<sup>6</sup> "Les figures politiques de la Privacy : Quels droits à la vie privée dans l'économie numérique?", à paraître

## RETRACER DES "LIGNES ROUGES"

---

Le fait d'identifier de nouveaux outils pour l'action des individus, ou de nouveaux leviers techniques et économiques d'intervention sur les décisions des acteurs, ne dispense pas de s'interroger également sur la nécessité, ou non, de tracer de nouvelles "lignes rouges", de redéfinir quelles pratiques sont dans tous les cas considérés comme graves et illicites.

La tâche est moins facile qu'il n'y paraît et nous ne pouvons ici qu'appeler à rouvrir la discussion sur ce thème, sans prétendre la clore par des recommandations formelles.

### Les lignes ont bougé

L'exemple des questions relatives aux orientations sexuelles, politiques et religieuses des utilisateurs de Facebook illustre la difficulté. Ces questions, donnant lieu à enregistrement dans un fichier et affichage sur une page de profil, sont clairement interdites par la loi française. Pourtant, elles constituent sans doute des critères essentiels pour les utilisateurs de Facebook à la recherche de nouvelles relations. Faut-il donc interdire à Facebook de poser ces questions qui font partie (aux Etats-Unis du moins) de son essence même ? Et par ailleurs, les données sensibles de 1978 et celles de 2008 sont-elles les mêmes ?

### Une clé : l'asymétrie d'information et de pouvoir

L'arbitrage effectué en 1978 se fonde sur le constat, peu contestable, d'une asymétrie d'information et de pouvoir entre l'individu isolé d'un côté, l'entreprise (fournisseur ou employeur) ou l'administration de l'autre. Dans certains cas, cette asymétrie conduit l'Etat à protéger l'individu contre lui-même, en fait contre ce qu'il pourrait être amené à faire sous la pression de ses interlocuteurs plus puissants. On ne peut pas lui poser certaines questions, même s'il est prêt à y répondre. Il ne peut pas vendre ses données, il n'en est pas propriétaire.

Faut-il remettre en question l'arbitrage de 1978, ou le revisiter ? Comment continuer de protéger les plus faibles contre les conséquences de leurs propres actes ? Y a-t-il de nouveaux risques de discrimination, de nouvelles données "sensibles" et d'autres qui ne le sont plus autant ? Faut-il abandonner certains champs naguère soumis à autorisation pour peut-être en investir d'autres, tels que ceux qui ont trait à la sécurité ou la santé "préventives" ?

Il semble difficile, au regard des changements que nous avons décrits plus haut, d'éluder ces questions, proprement politiques.

## CONCLUSION PROVISOIRE

Les principes d'"Informatique et libertés" demeurent valides après 30 ans. Ses modalités d'application ont déjà beaucoup changé. Mais aujourd'hui, le changement nécessaire paraît plus profond encore.

Dans son étude citée plus haut, l'institut Demos exprime assez brutalement que *"la question n'est pas de savoir si nous entrons dans une société dominée par la surveillance, mais s'il en résulte davantage, ou moins, de contrôle des individus sur leur propre vie, ainsi que sur les décisions d'intérêt collectif."*

C'est dans cet esprit que nous avons tenté de dégager les nouveaux défis de la protection et de la négociation des données personnelles, en tenant compte des aspirations et des pratiques réelles de la société et des organisations, et en ouvrant des pistes nouvelles.

La tâche des humains est à la fois de créer les systèmes techniques qui soutiennent leurs civilisations, et d'en borner le champ, d'en réguler le fonctionnement. Ils le font lors de leur conception, en définissant leur architecture, et plus tard, en imposant des règles et des contrôles. Mais ils le font aussi tous les jours, quand ils changent d'avis, trichent, bricolent, se trompent, renégocient, mentent...

Ces deux plans, général et politique d'une part, quotidien et économique de l'autre, doivent aujourd'hui s'agencer d'une manière qui demeurerait inconcevable en 1978, lorsque l'usage des outils numériques était réservé à quelques professionnels.

Au fond, c'est ce qu'il nous semble ressortir de plus fort dans les réflexions du groupe de travail : l'idée que la protection de la vie privée, conçue comme un édifice juridique fonctionnant par défaut et pour tous, doit désormais se compléter de dispositifs de "maîtrise", plus complexes et mouvants, qui permettent aux individus – dans des limites à mieux définir – d'organiser à leur manière ce qu'ils veulent défendre, ce qu'ils veulent exposer et ce qu'ils sont prêts à négocier. Et aussi, de dispositifs collectifs mais non étatiques, capables d'exercer des formes de pression que l'Etat ne parvient pas (ou plus) à exercer.

Cette nouvelle architecture de protection et de maîtrise n'émergera pas toute seule. Il y a des recherches à entreprendre, des idées à explorer, des innovations à tester ou promouvoir, des services et des médiations à créer, des débats à mener. Certains sujets seront presque consensuels, d'autres carrément conflictuels.

Il faut choisir de s'engager sur ce chemin. L'immobilisme n'est pas une option.

Et il faut s'y engager ensemble. De ce point de vue, notre message ne s'adresse pas uniquement aux institutions ou aux activistes. Les entreprises seraient bien inspirées d'explorer elles aussi les pistes que nous avons tenté de défricher, et d'autres, pour éviter à terme une rupture grave de la confiance.