

TRACES NUMÉRIQUES ET PROTECTION DES DONNÉES PERSONNELLES : LES NOUVEAUX ENJEUX

Alex Türk, Sénateur du Nord, est président de la CNIL depuis 2004. Il préside également le G29, groupe des "CNIL européennes".

Résumé : Nous n'en avons pas nécessairement conscience, mais volontairement ou non, nous laissons derrière nous des traces qui permettent à autrui de nous suivre de plus en plus finement, dans l'espace comme dans le temps, en tissant autour de nous un maillage d'informations révélatrices de notre activité, de notre vie privée, de notre personnalité. La question est de savoir comment définir et réguler la protection de la vie privée face au développement permanent des technologies et des mentalités. C'est le défi auquel la commission nationale de l'informatique et des libertés (CNIL) est confrontée en permanence, et tout particulièrement aujourd'hui.

Abstract : *We may not be aware of this, but willingly or not, we leave traces behind us that enable others to follow us more and more accurately, in space and time, by weaving a mesh of relevant information on our activity, our private lives, our personalities. The question is to know how to define and regulate the protection of our private lives in view of the constant development of technologies and mentalities. That is the challenge the French Commission Nationale de l'Informatique et des Libertés (CNIL - IT and liberty national commission) is constantly facing and particularly today.*

Traduire la complexité du monde dans un projet culturel associant les sciences et les sociétés » : telle est l'ambition affichée par le Musée des Confluences.

Un tel dessein ne peut, à l'évidence, s'affranchir d'une réflexion profonde relative à l'impact des nouvelles technologies sur la société, et tout particulièrement à celui de la traçabilité numérique des individus qui la composent. Pas davantage, en effet, que les autres sociétés du monde moderne, la société française n'a encore pris la pleine mesure de ce phénomène.

Qu'est-ce que la traçabilité numérique, et quels sont les risques ?

Nous n'en avons pas nécessairement conscience, mais volontairement ou non, nous laissons derrière nous des traces qui permettent à autrui de nous suivre de plus en plus finement, dans l'espace comme dans le temps, en tissant autour de nous un maillage d'informations révélatrices de notre activité, de notre vie privée, de notre personnalité – autant d'éléments constitutifs, in fine, de notre identité et de notre intimité¹.

Tel est, bien sûr, le cas quand nous utilisons notre carte bancaire, notre téléphone portable, notre passe électronique dans les transports, ou lorsque nous avons recours à un service de télépéage. Dans toutes ces hypothèses, la technologie gardera mémoire de ces traces et permettra alors à d'autres que nous de dire, précisément, où nous étions et à quelle heure, de même que la durée de notre trajet, le montant et la nature de nos achats, selon les circonstances, etc.

Il en est également ainsi, de manière plus insidieuse, des applications qui permettent de collecter des traces de nos déplacements sans que nous les ayons délibérément provoquées. Il suffit d'évoquer le développement de la biométrie, de la géolocalisation ou de la vidéosurveillance ou encore, plus récemment, l'apparition de la notion « d'Internet des objets » : ce développement des systèmes qui permet de lier un objet à Internet, comme un vêtement ou un livre par exemple, en lui associant une étiquette

munie d'un code ou d'une adresse URL, qui sera ensuite lue par des capteurs mobiles sans fil atteignant, à terme, l'échelle nanométrique. Autant d'usages de la technologie qui permettent de nous suivre dans l'espace,

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004, qui la qualifie d'autorité administrative indépendante.

Une autorité indépendante
L'indépendance de la CNIL est garantie par sa composition et son organisation. Ainsi, douze des dix-sept membres qui composent la CNIL sont élus par les assemblées ou les juridictions auxquelles ils appartiennent.

- La CNIL élit son Président parmi ses membres ;
- elle ne reçoit d'instruction d'aucune autorité ;
- les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent s'opposer à l'action de la CNIL pour quelque motif que ce soit et doivent prendre toutes mesures utiles afin de faciliter sa tâche.

Le Président de la CNIL recrute librement ses collaborateurs.

¹ : L'augmentation du traçage est également constatée et analysée par le Sénat dans son rapport relatif au respect de la vie privée à l'heure des mémoires numériques, présenté en commission des Lois le 27 mai 2009 et disponible à l'adresse suivante : <http://www.senat.fr/rap/r08-441/r08-4411.pdf>.

le plus souvent à notre insu, lors de nos déplacements, de nos actes d'achat, de nos activités, de nos loisirs et qui permettent de cerner peu à peu notre comportement et nos habitudes de vie.

Quant à Internet, il génère, à lui seul, une mine d'informations phénoménale, susceptible d'exploitations infinies.

La traçabilité numérique est inhérente à l'utilisation du « réseau des réseaux » : le simple fait de se connecter à un site, de participer à des réseaux sociaux, d'utiliser un moteur de recherche, offre autant d'occasions d'être tracés, non plus tant alors dans l'espace que dans le temps.

Car lorsqu'il y a diffusion de données sur Internet, il y a également conservation et réutilisation à toutes fins de celles-ci par autrui, qu'il s'agisse de ses amis, de « sa » communauté (qui peut être celle de plusieurs millions d'internautes !), des sites et de leurs multiples partenaires commerciaux, de son futur employeur peut-être, sans oublier, dans des hypothèses alarmistes mais réelles, l'éventualité de voir son identité usurpée par autrui.

Or, contrairement à une idée courante, nos traces ne sont pas anodines. Elles le sont d'autant moins qu'il est aujourd'hui difficile, parfois même impossible, de retirer complètement l'information du Web une fois qu'elle est publiée : même après suppression sur le site d'origine (par exemple celui d'un réseau social), des copies peuvent être conservées chez des tiers ou des prestataires de service de réseaux sociaux. De surcroît, cette traça-

bilité numérique est omniprésente puisque, à l'enregistrement des actions des internautes dès qu'ils utilisent un service, s'ajoute la conservation des données de connexion par les opérateurs, pour des raisons légales².

Soulignons, à cet égard, que ce potentiel de traçabilité a été décuplé à l'avènement du Web 2.0, qui a consacré la dualité de la nature de l'internaute : celui-ci est à la fois un « ficheur », qui génère et diffuse des informations sur lui-même et sur les autres, et un « fiché » qui, consciemment ou non, génère des traces qui le transforment en une cible privilégiée des stratégies d'analyse comportementale, notamment à des fins de marketing.

Pourtant ces réalités, progressivement admises, n'atténuent généralement pas l'engouement des personnes pour les nouveaux services gratuits qui collectent et exploitent leurs données personnelles, parfois aux dépens du respect de leur vie privée. La traçabilité semble alors être un fait inéluctable.

Dès lors, comment éviter que l'on sache tout de nos goûts vestimentaires, de nos choix de lecture, de notre réseau relationnel, de notre recherche d'emploi ? Comment éviter que le film d'une soirée plutôt arrosée, posté sur un site vidéo, que la confiance livrée, à 16 ans, sur Internet, à propos de préférences sexuelles, ou une attirance pour tel ou tel mouvement extrémiste soient ressortis lors d'un entretien de recrutement ? Comment, finalement, se soustraire à un tel « profilage » social et économique, maîtriser l'utilisation de ses données, préserver, pour chacun d'entre nous, le droit à l'oubli et à une vie privée ?

2 : Cf. la loi sur la confiance dans l'économie numérique, le code des postes et des communications électroniques ou la directive européenne sur la conservation des données.

Ces questions délicates posent, au fond, la question de savoir comment définir et réguler la protection de la vie privée face au développement permanent des technologies et des mentalités, à une époque où vie privée et espace public s'interpénètrent jusqu'à ne former plus qu'un.

C'est le défi auquel la Commission nationale de l'informatique et des libertés (CNIL) est confrontée en permanence, et tout particulièrement aujourd'hui.

La vigilance de la CNIL face aux nouvelles technologies

Il est utile de rappeler, au préalable, que l'article 1^{er} de la loi « informatique et libertés », dispose que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Depuis 1978, notre commission a donc pour mission de garantir que les technologies se développent dans le respect des principes de protection des données, lesquels participent des droits et libertés fondamentales des citoyens.

Mais dans l'environnement en constante évolution évoqué plus haut, une telle vocation a-t-elle encore un sens ? Finalement, la notion de vie privée n'a-t-elle pas progressivement disparu au profit de celle de transparence de l'individu ? N'est-il pas illusoire de chercher à protéger la vie privée dans un monde où l'exposition de l'intime est devenue banale, où la technologie est devenue invisible et dispersée ?

Loin d'être périmés, les principes de protection de la vie privée et des données personnelles sont, bien au contraire, plus pertinents que jamais.

Les règles de protection des données protègent des personnes.

Il s'agit de protéger un droit à ne pas être fiché, surveillé, tracé, contrôlé de manière abusive et incontrôlée ; il s'agit de protéger la dignité humaine, de permettre aux personnes d'exercer leurs droits et que leurs intérêts légitimes soient préservés.

Il ne s'agit pas de condamner la technologie dans un emballement rétrograde, mais de faire comprendre que l'innovation technologique est porteuse à la fois de progrès et de dangers. Car autant les individus sont tentés par le confort qu'elle procure, autant ils sont peu conscients des risques qu'elle comporte. Cette tâche est d'autant plus urgente que le progrès technologique est irréversible : nous ne vivrons plus jamais dans un monde sans ordinateurs, sans Internet, sans téléphones portables, sans identification biométrique, sans géolocalisation, sans vidéosurveillance. Ces technologies tendent au contraire à s'imbriquer les unes dans les autres, et les synergies qu'elles créent sont des plus dangereuses pour nos sociétés.

Nous nous attachons donc à être particulièrement vigilants à l'égard des risques qu'induit le développement technologique envers les droits et libertés des personnes. À cette fin, nos moyens d'action sont diversifiés.

Actions de sensibilisation, campagnes d'information

Notre commission est constamment, et de plus en plus, engagée dans un puissant effort de pédagogie visant à informer les personnes de l'existence et du contenu de leurs droits.

L'axe prioritaire doit être l'action à destination des enfants et adolescents,

qui constituent sans doute la population la plus vulnérable, tant est grande leur méconnaissance vis-à-vis des risques induits par les nouvelles technologies. Ainsi, à titre d'exemple, notre commission a signé une convention de partenariat avec la Défenseure des enfants en vue de proposer aux jeunes d'adopter de bonnes pratiques et d'améliorer la connaissance de la loi « informatique et libertés » auprès des parents, enseignants, ou éducateurs. Elle est également membre du comité de pilotage du programme « Internet sans crainte », le volet national du programme européen Safer Internet, qui a notamment financé le dessin animé Vinz et Lou à destination des 7-12 ans. Enfin, dans le même esprit, nous nous apprêtons, au début de l'année 2010, à publier une édition spéciale d'un quotidien à destination des enfants. Nous serons également partenaires d'un serious game pour les adolescents, qui pointe, de façon ludique, les conséquences futures de certaines traces laissées sur le Web. Un clip de sensibilisation sera disponible sur le Web, et une rubrique modernisée sur son site Internet, intégralement dédiée aux traces, permettra aux enfants de comprendre la manière dont cette traçabilité opère lorsqu'ils « se déplacent » sur le Web.

L'industrie qui conçoit les technologies de demain

constitue, bien évidemment, une autre cible privilégiée. Notre commission a ainsi mis en place un service d'expertise technologique de haut niveau qui lui permet, entre autres, de s'insérer efficacement dans les cursus de formation des futurs ingénieurs pour les sensibiliser aux principes de protection des données.

De même, nous encourageons activement les entreprises établies en France à se doter d'un **correspondant « informatique et libertés »**, qui veillera à diffuser cette culture au sein de leur structure.

Notre commission contribue enfin aux débats publics lancés sur le plan national.

Ainsi, un débat public national est organisé depuis l'automne 2009 au sujet des nanotechnologies, sous la forme de réunions publiques dans plusieurs grandes villes, et de forums de discussion. Nous y participons pour sensibiliser les personnes et les pouvoirs publics aux risques que ces technologies comportent en matière de systèmes d'informations.

Les moyens effectifs d'intervention : une doctrine d'application concrète, des pouvoirs contraignants.

Depuis sa création en 1978, notre commission s'est toujours attachée à élaborer une doctrine concrète et pragmatique, qu'elle n'a pu longtemps mettre en œuvre qu'en déployant des trésors de pédagogie. En 2004, la loi a radicalement changé la donne en la dotant d'outils extrêmement puissants, comme son pouvoir étendu de contrôle et de sanction encadré par le juge (possibilité de diligenter des vérifications sur place, de prononcer une mise en demeure, d'imposer des sanctions pécuniaires, des avertissements, le verrouillage de fichiers, etc.).

C'est en faisant usage de toute la gamme de nos pouvoirs que nous encadrons les dispositifs de traçabilité informatique des personnes.

Une action résolument européenne et internationale

Mais une action limitée au niveau national n'aurait guère de sens dans un monde global, face à des technologies d'application planétaire. L'action nationale de la CNIL se complète donc naturellement par des travaux intensifs sur le plan international.

Depuis 15 ans environ, notre commission et ses homologues européens, regroupés au sein d'un groupe dit « de l'article 29 » (ou G29), que je préside actuellement, travaillent de manière concertée sur les sujets technologiques. Ces travaux européens sont totalement cohérents avec ceux menés par la Conférence mondiale des commissaires à la protection des données, qui réunit annuellement près de 80 autorités de protection des données, mais également de nombreux représentants de la société civile, de l'industrie mondiale, de cabinets d'avocats internationaux, et d'autres autorités publiques.

Les problématiques de traçabilité numérique sont régulièrement évoquées dans ces enceintes, qui sont ainsi devenues, pour les industries concernées, un interlocuteur institutionnel incontournable.

S'agissant des **moteurs de recherche**, tout d'abord, le G29 a certes reconnu l'utilité de ces outils, mais aussi publiquement identifié les nouveaux risques qu'ils engendrent. Il a ainsi précisé les règles qui doivent leur être applicables dans un avis d'avril 2008 ³, en préconisant en particulier la réduction à six mois de la durée de conservation des données qu'ils collectent sur leurs utilisateurs.

S'agissant des **réseaux sociaux**, le G29 a établi une réglementation applicable en la matière dans un avis du 12 juin 2009, en affirmant que les règles européennes de protection des données et de la vie privée s'appliquaient aux réseaux sociaux, même quand leur siège se trouve hors d'Europe. Cette affirmation peut sembler de bon sens, tant il est légitime que des règles visant à protéger les citoyens européens s'appliquent à des

services qui collectent et traitent les données intimes de millions d'entre eux. Pourtant, rares sont, en pratique, les entreprises américaines qui acceptent d'appliquer ces principes spontanément. Ainsi, faire valoir l'impératif de proportionnalité des données collectées par rapport à la finalité du service rendu, rendre effectif le droit d'opposition des citoyens européens à figurer dans un fichier, limiter la durée de conservation de leurs données dans les bases informatiques situées aux États-Unis, vérifier l'encadrement des conditions juridiques et techniques de ces transferts sont autant de combats quotidiens pour la CNIL et ses homologues européens.

Quelle gouvernance internationale, quelle vision pour demain ?

La révolution technologique mondiale à laquelle nous assistons aujourd'hui impose de transcender les moyens d'action dont disposent actuellement les autorités comme la CNIL. Face aux géants américains de l'Internet qui se sentent rarement concernés par les lois européennes, lesquelles sont les plus protectrices au monde, nous avons besoin d'instruments qui dépassent les règles nationales et les résolutions sans force légale pour imposer notre vision humaniste.

C'est pourquoi la conférence mondiale de Madrid a adopté, le 6 novembre 2009, une résolution visant à établir des standards internationaux sur la protection des données personnelles et de la vie privée. L'adoption

3 : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_fr.pdf.

d'un tel document constitue un pas historique : pour la première fois, les autorités de protection des données sont parvenues à élaborer au niveau mondial un corpus de principes communs adaptés aux dernières évolutions technologiques.

L'objectif de ces différentes démarches est à la fois ambitieux et déterminé : il s'agit de pousser à l'adoption d'instruments juridiques contraignants qui sécuriseront la protection de la vie privée des citoyens européens sur le plan international. Ne nous voilons pas la face : cette seconde étape sera plus longue et plus difficile.

Toutes ces actions et ces évolutions sont à la fois porteuses de sens et concrètes mais elles ne se substitueront jamais à la conscience des personnes quant aux risques qu'elles prennent en acceptant leur traçabilité numérique comme une banalité, un fait inéluctable.

Le parallèle qui me paraît le plus pertinent pour appeler à cette prise de conscience est tiré de la protection de l'environnement : de même que nous prenons progressivement conscience du danger vital auquel est exposé le

capital de notre planète, de par la pollution issue de l'activité humaine, nous devons également prendre conscience des dangers qu'encourt aujourd'hui notre « capital de libertés ».

À l'instar de la mesure de l'empreinte carbone des techniques utilisées par l'homme, c'est-à-dire de leur impact sur l'environnement, pourquoi ne pas évaluer le potentiel de nocivité des technologies en tenant compte de leur « empreinte informationnelle », résultat de leur potentiel de traçabilité dans l'espace et dans le temps ?

Car la protection des données est peut-être aussi précieuse que l'air que nous respirons : tous deux sont invisibles, mais les conséquences sont tout aussi désastreuses quand l'une ou l'autre vient à manquer.

Chacun doit être conscient que ce qui légitime le principe de la protection des données personnelles n'est ni plus ni moins que la recherche des moyens de garantir, au sein de la civilisation numérique dans laquelle nous entrons, nos deux plus précieux droits : la liberté d'aller et venir et la liberté d'expression.