INSTITUT DIDEROT

Les Carnets des Dialogues du Matin

ALEX TÜRK

L'avenir de la vie privée dans la société numérique

www.institutdiderot.fr

Les Carnets des Dialogues du Matin

ALEX TÜRK

L'avenir de la vie privée dans la société numérique

Sommaire

Avant-propos
Dominique Lecourt p. 5

L'avenir de la vie privée
dans la société numérique
Alex Türk p. 7

Les publications
de l'Institut Diderot p. 29

Avant-propos

Voici un appel à la réflexion et à l'action face au « déferlement numérique » auquel nous assistons trop passivement. Cet appel émane de celui qui de 2004 à 2011 a présidé la Commission nationale de l'informatique et des libertés (CNIL).

Il s'appuie sur des exemples concrets empruntés à ces grands domaines que sont la vidéosurveillance, la biométrie, la géo-localisation et le réseau informatique mondial.

La vie privée et l'intimité des citoyens se trouvent indéniablement menacées ; la majorité des internautes n'a pas conscience de l'utilisation possible, grâce à l'évolution extrêmement rapide des technologies, de ses données personnelles par les grands acteurs de l'Internet ou par un gouvernement. Mais Alex Türk n'est pas un penseur catastrophiste. Il ne dénigre pas les technologies nouvelles ou l'intelligence créative des grands noms du web. Aucune fin du monde n'est annoncée. En revanche, l'ancien président de la CNIL avance des solutions pour mieux protéger la liberté des citoyens. On ne s'étonnera pas que ces solutions reposent en définitive sur la prise de conscience et la mobilisation de tous.

Pr. Dominique Lecourt
Directeur général de l'Institut Diderot

L’avenir de la vie privée dans la société numérique

C’est à titre personnel, puisque je ne suis plus désormais président de la CNIL, que je souhaiterais exprimer, dans ce carnet, un certain nombre de préoccupations.
J’ai choisi de ne traiter ici que d’un seul sujet : celui du déferlement des technologies du numérique. On pourrait tout aussi bien écrire un autre texte sur la problématique des *fichiers* : problématique qui paraît plus classique mieux connue, mais qui demeure néanmoins extrêmement importante et doit servir de toile de fond aux réflexions que je vais développer ici. J'aime évoquer à cet égard l'exemple du président actuel du groupe des 27 CNIL européennes, qui avait, un jour, demandé à ses collaborateurs de déterminer précisément dans combien de fichiers il se trouvait. L'étude établit qu'il était inscrit dans près de 400 fichiers, soit régaliens, soit du secteur privé. J’aime évoquer à cet égard l’exemple du Président actuel du groupe qui réunit les 25 CNIL européennes. Il avait demandé un jour à ses collaborateurs de déterminer précisément dans combien de fichiers il se trouvait. L’étude établit qu’il était inscrit dans près de 400 fichiers… On considère d’ailleurs, plus généralement, qu’une personne menant une vie sociale « moyenne » voit ses coordonnées reprises dans environ 400 fichiers : elle s’y

trouve dans certains en le sachant et dans d'autres cas à son insu, parfois avec son accord, parfois non. Il faut donc bien situer tout ce que je vais exposer à l'intérieur de ce contexte général : nous sommes désormais tous saisis, encadrés, entourés par une multiplicité de fichiers dont nous ignorons souvent tout.

Au demeurant, cela ne signifie absolument pas que je conteste *en soi* la légitimité de l'existence de ces fichiers. Je ne revendique, en aucun cas, l'arrêt du développement de ces fichiers ou du développement technologique en général. C'est d'ailleurs pour cette raison que les décisions à prendre sont toujours complexes. Dans beaucoup d'hypothèses il me semble que l'objectif recherché en mettant en place ces fichiers est parfaitement justifié : la société, dans tel et tel cas, a raison de développer telle technologie pour atteindre telle finalité. Mais pour atteindre cette finalité, on soulèvera d'autres problèmes et ma question est : ces autres problèmes ont-ils fait l'objet d'une évaluation ?

Ce qui me conduit à une seconde remarque introductive : il n'existe pas de bonne ou de mauvaise technologie *en soi.* Rien n'est plus absurde que de vouloir qualifier une technologie, en tant que telle. Si on prend n'importe quelle technologie, aujourd'hui en application, on lui trouvera nécessairement à la fois des effets qui paraîtront négatifs et d'autres positifs, l'appréciation que l'on porte sur ces effets pouvant d'ailleurs varier selon les époques, de même que les effets eux-mêmes. Il convient donc de s'inscrire dans cette *relativité* pour éviter de tomber dans l'excès. C'est d'ailleurs souvent bien difficile à faire comprendre. Je me rappelle, par exemple, un journaliste qui me sollicita car il souhaitait publier un article sur la biométrie. Il avait, disait-il, trouvé quelqu'un qui était « pour » la biométrie

et voulait que je lui dise que j'étais « contre ». Je lui répondis que je n'étais ni pour, ni contre, et que tout dépendait de quelle biométrie il s'agissait, dans quel cas, dans quel contexte etc. Dépité, il me dit qu'il irait solliciter quelqu'un d'autre… Comme Président de la CNIL, je considérais absurde d'accepter de me prêter à un tel exercice. Une fois ces points mis au clair, venons-en au problème qui m'occupera dans ce texte.

Je commencerai par décrire les principales technologies qu'on peut regrouper sous le titre de « technologies du numérique ». J'en exposerai ensuite les principaux risques à court et moyen terme. Puis j'essaierai de montrer quels types de solutions permettraient de juguler ou de contrôler au minimum certains de ces risques. Ma conviction, en effet, est qu'il est *encore possible*, par une action volontariste, de réduire certains des risques associés aux technologies du numérique. Mais cela requiert au préalable d'en prendre conscience et d'informer le public sur ces questions trop peu souvent discutées.

1. QUELLES SONT LES TECHNOLOGIES MISES EN ŒUVRE ?

Nous en retiendrons quatre.

A. La vidéosurveillance.

Il peut paraître curieux de faire figurer la vidéosurveillance dans les technologies du numérique. Cependant, si encore récemment cette technologie reposait sur un système analogique, elle s'appuie désormais à près de 99%, sur le numérique. Cette technologie pose un certain nombre de problèmes, mais on peut assez aisément les encadrer ou

les juguler parce qu'ils sont assez bien connus et que le cadrage juridique est assez précis, fonctionnel et concret. Nous parlons là de la vidéosurveillance *seule*. Car lorsqu'elle entre en synergie avec d'autres technologies, les choses deviennent plus complexes. Nous y reviendrons.

En outre, l'un des grands avantages de la vidéosurveillance est qu'elle fait partie du groupe des technologies numériques dont on *pourrait* décider (ce qu'on ne fera jamais…) de les *abandonner totalement*. En effet, parmi les quatre technologies que je vais évoquer, les deux premières (vidéosurveillance et biométrie) pourraient ne plus être appliquées du jour au lendemain, si une décision était prise en ce sens par les pouvoirs publics d'un État souverain. En revanche, pour les deux dernières (géo-localisation des personnes et des biens et « réseau internet »), les choses sont très différentes : on peut toujours souhaiter les abandonner mais comme il s'agit de phénomènes planétaires et trans-étatiques, on ne dispose pas, en réalité, de la maîtrise de la décision. Décider demain d'interdire la géo-localisation ou le réseau internet sur le territoire français, cela n'aura guère d'effet...

B. La biométrie

La biométrie est un cas particulier en France car, pour la mettre en place, il faut obligatoirement avoir l'accord de la CNIL. Celle-ci a en effet ici un pouvoir d'*autorisation*, en particulier pour le secteur privé.

La biométrie implique d'utiliser un élément du corps humain pour fixer, reconnaître ou déterminer l'identité d'une personne. En la matière, il n'y a pas de limites à l'imagination humaine. Aujourd'hui, on fait ainsi de la biométrie à partir de tous les éléments du corps humain : par exemple, la silhouette d'un corps, sa manière de se

mouvoir, son odeur[1]. Si on se limite aux hypothèses les plus classiques, on utilisera ou bien l'œil (la rétine, l'iris ou la cornée[2]), ou bien la main. L'utilisation de la main est encore aujourd'hui la plus courante. Trois possibilités sont alors envisagées. 1. La reconnaissance du *contour géométrique de la main ouverte*. Un appareil est ainsi de capable de reconnaître la forme d'une main parmi des centaines de milliers d'autres. Seulement, lorsqu'on ferme le poing, la trace de la main ouverte disparaît… 2. L'utilisation de *l'empreinte digitale numérisée* : cette fois, la trace reste, par exemple sur des objets (un verre, une porte etc.). Si bien que si quelqu'un de malintentionné le souhaite, il peut prendre le verre dans lequel j'ai bu et usurper mon identité, à travers un modelage de mon index, pour accéder à un endroit sécurisé. 3. L'utilisation du *réseau veineux de la paume de la main ou de l'index*. Système très prometteur car il présente une différence importante par rapport au précédent: je ne laisse pas la trace de mon réseau veineux sur un verre. En revanche, on obtient un taux de fiabilité comparable à celui de l'empreinte digitale, soit près de 99%.

Comment faire le tri entre ces différentes techniques ? Un exemple nous aidera à répondre à cette question. Il y a 7 ou 8 ans, la CNIL avait accepté de traiter le problème posé

1. C'est le cas par exemple en Corée où l'on a développé des techniques de reconnaissance des personnes à leur odeur, indépendamment même du fait qu'elles portent ou non une eau de toilette.

2. Il semble qu'aujourd'hui ce soit l'iris qui apparaisse le plus fiable. Lorsque j'ai été élu président de la Cnil, les ingénieurs affirmaient ne pouvoir reconnaître l'iris qu'à 50 cm de distance. Désormais, des études au Mexique, par exemple, permettent de le reconnaître à plus de vingt mètres. Tôt ou tard, on saisira l'iris d'une personne au vol dans la rue à 50 ou 100 mètres. Il n'y a certainement pas beaucoup de limites en la matière.

par un certain nombre de responsables d'établissements scolaires qui souhaitaient utiliser une biométrie pour contrôler l'accès aux réfectoires. Actuellement, plus de 400 établissements, en France, utilisent ce système. La CNIL s'était alors absolument opposée à l'usage de l'empreinte digitale numérisée, mais elle a accepté (on peut d'ailleurs discuter cette décision) que soit utilisé le contour géométrique de la main ouverte. Pour l'élève, la différence, en pratique, est faible : il présente sa main et non pas son seul index à l'appareil. Mais en vérité, elle est considérable : il n'y a pas de possibilité de dérives avec le système à main ouverte ; il pourrait y en avoir avec l'empreinte digitale numérisée.

La décision de la CNIL était motivée par le fait que nous ne voulions pas courir le risque de nous retrouver ensuite avec des milliers de fichiers d'empreintes d'adolescents dispersés dans la nature, sans véritable encadrement juridique. D'autant que l'on obtenait un résultat comparable, avec un risque nul, avec le système main ouverte. Il est vrai que sa fiabilité est actuellement plus faible. Mais l'enjeu, en termes de sécurité, de la vérification de l'identité d'un élève qui entre au réfectoire n'a rien de comparable avec celui qui se pose, par exemple, pour contrôler l'accès au tarmac de Roissy ou à un laboratoire qui manie des produits toxiques. Il était donc légitime de mettre en place un raisonnement en termes de proportionnalité, qui évalue les rapports bénéfices-risques dans les différents cas. Il nous a donc semblé que, pour vérifier si un élève peut entrer au réfectoire et a bien payé sa cotisation, on peut se contenter d'un système moins fiable (étant donné les risques que présente le système alternatif en termes de circulation de fichiers) tandis qu'on ne peut pas se contenter d'une fiabilité incertaine pour vérifier qui accède au tarmac de Roissy.

Au cas où l'on douterait de la réalité du danger qui tient à l'utilisation d'une empreinte numérisée, cette anecdote peut servir d'illustration. Régulièrement, lorsque nous faisions des réunions à la CNIL, la question de la réalité d'un risque d'usurpation d'identité par utilisation de l'empreinte numérisée revenait. Un jour, nous avons donc demandé au responsable de notre service d'expertise technologique de nous faire une démonstration sur ce point. Il me demanda de quel budget il pouvait disposer. Par boutade, je lui répondis : « 25 euros. » Il me prit au mot et m'assura qu'un tel budget lui suffisait amplement. Nous avons donc loué un système biométrique d'accès par reconnaissance digitale qui permettait l'ouverture d'une porte sur présentation du doigt d'une personne préalablement enregistrée. Nous avons demandé à une collaboratrice de laisser un verre dans lequel elle avait bu et l'ingénieur l'a récupéré. Le challenge consistait à ouvrir la porte à partir de ce seul verre, étant entendu que seule notre collaboratrice avait été enregistrée dans le système biométrique contrôlant son ouverture. L'ingénieur est simplement allé acheter de la pâte à modeler et une bouteille de latex liquide blanc, soit moins de 25 euros. Avec ce matériel et celui à disposition de la CNIL (un crayon et une photocopieuse), il a pu confectionner un faux doigt en latex avec lequel il a effectivement réussi à ouvrir la porte. Il avait donc réussi à usurper l'identité de sa collègue sans aucune difficulté. Il faut certes reconnaître que l'appareil dont nous disposions était assez simple ; mais il est vrai aussi que le budget que nous avions dépensé pour le mettre en échec était dérisoire. Il y avait donc, là encore, une certaine proportionnalité. La sécurité absolue n'existant pas, on considère d'ailleurs généralement que le taux de sécurité ultime est atteint lorsque, pour

« craquer » le système d'un Etat, il faut mobiliser les moyens d'un autre Etat de puissance comparable.

Quelle leçon tirer de cette expérience ? S'il s'était agi, dans le réel, d'une usurpation concernant un ingénieur, membre d'une équipe travaillant sur un projet dans un domaine sensible, la première constatation serait de relever un grave défaut de sécurité du système. Deuxièmement l'intéressé serait ainsi placé dans une situation très délicate car il serait dans l'incapacité de démontrer qu'il n'est pas en cause dans l'intrusion. Enfin on imagine aisément les possibilités de détournement ainsi offertes à de « mauvais esprits » au détriment de leurs congénères !

L'utilisation de la biométrie se fait donc, sous le contrôle de la CNIL, en fonction d'un raisonnement de proportionnalité qui conjugue les notions de fiabilité, de sécurité et de protection de la vie privée.

Je prendrai sur ce point un dernier exemple pour montrer la complexité des décisions dans certains cas. Il y a un an, le centre Oscar Lambret de Lille, centre de recherches avancées en matière de lutte contre le cancer, a déposé un dossier auprès de la CNIL, suite à un certain nombre d'affaires tragiques qui avaient eu lieu à l'hôpital d'Épinal, où des erreurs d'identité avaient abouti au décès de plusieurs patients par surdose lors de radiothérapies. Le centre avait demandé à se doter, pour éviter ce genre de problèmes, d'un système biométrique à l'entrée de la salle de radiothérapie, afin de vérifier automatiquement qu'il s'agissait du bon patient. Pour ce faire, il souhaitait utiliser un système à empreinte digitale numérisée. Après deux heures de débats sur le sujet, les membres de la CNIL n'ont pas réussi à s'entendre sur le sujet. Nous étions très partagés et nous nous demandions notamment s'il ne valait pas mieux utiliser le système reposant sur le réseau veineux,

dont nous avons vu qu'il est presque aussi fiable que l'empreinte digitale, mais qu'on ne peut le détourner aussi facilement que cette dernière. Nous avons formulé une réponse en ce sens au centre et invité son directeur à venir en débattre. En dix minutes, la question fut réglée car il nous expliqua que, s'il comprenait bien notre position, il ne pouvait pas, malgré tout, utiliser le réseau veineux parce que le centre soignait certaines affections dans lesquelles celui-ci était endommagé par les soins et qu'en conséquence, il ne pourrait être fiable. Immédiatement, nous avons donné notre accord parce qu'était ainsi apportée une réponse très concrète qui faisait basculer en ce sens le calcul de proportionnalité.

C. La géo-localisation

Cette technologie consiste à suivre une personne à la trace en différé ou en direct par divers moyens. On peut distinguer entre les cas où on fait de la géo-localisation *par effet et non pas objet* : par exemple, lorsqu'on utilise une carte bancaire, on en attend un service financier ; lorsqu'on utilise un téléphone portable, on en attend un service de communication, etc. Mais, dans chaque cas, l'un des *effets* du service est que l'on peut être ainsi suivi à la trace. Dans d'autres cas, la géo-localisation est *l'objet même de la technologie* : c'est le cas des systèmes GPS ou des puces RFID. Dans ces cas, on utilise la technologie *pour suivre* une personne et la repérer dans l'espace. Il existe alors des cas où cette volonté de géo-localisation est elle-même *subordonnée à un objectif autre* : par exemple, on peut équiper un camion livreur de fuel d'un système GPS pour repérer où il se trouve et améliorer ainsi les coûts logistiques d'une PME. Dans d'autres cas, on géo-localise pour *géo-localiser* : ce sont les cas où on utilise ces systèmes pour suivre les

gens, voir ce qu'ils font, les entendre et les enregistrer. Dans ces cas, on peut parler de « *géo-localisation par objet au carré* ». Prenons quelques exemples pour illustrer, là encore, les problèmes très différents qui peuvent se poser selon les cas dans l'utilisation de ces technologies. On se sert par exemple de la géo-localisation pour assister certaines catégories de personnes qui manquent d'autonomie : c'est le cas en particulier *dans les maternités pour la surveillance des nourrissons*. On définit un périmètre de 50 ou 100 m autour du lieu où se trouvent les bébés et on équipe ces derniers d'une technologie de géo-localisation – par exemple un bracelet. Si l'enfant franchit le périmètre déterminé, une alarme se déclenche. Ces systèmes, qui se développent énormément actuellement, permettent aux maternités de rassurer les parents quant à la protection de leurs nourrissons.

De nombreux dossiers nous ont été transmis en ce sens. Pour les traiter, nous avons regardé les statistiques de disparitions d'enfants dans les maternités. Nous avons ainsi appris qu'il y en avait environ 1,6 par an, dont 1 en moyenne était retrouvé ! Le taux de disparition de nourrisson est donc extrêmement faible. C'est déjà trop, bien sûr, mais enfin on ne peut pas considérer qu'il s'agit là d'un objet social actuellement fondamental. Ce type d'informations n'est certes pas suffisant mais il permet au moins de nuancer les affirmations des vendeurs de ces systèmes, qui promeuvent leurs produits en évoquant le « développement considérable » des enlèvements de nourrissons dans les maternités ces dernières années…

Mais il convient d'aller plus loin : que se passe-t-il si la personne qui est en charge du système d'alarme est défaillante elle-même ? Dans ce cas, il n'y a plus de surveillance du tout puisque l'on a expliqué aux jeunes

mères que l'on surveillait leurs enfants à leur place. Et plus profondément se pose ici un problème pédagogique : est-il vraiment pertinent de dire à une jeune maman qui vient d'accoucher : « ne vous inquiétez de rien, pendant les quatre-cinq jours que vous passerez à la maternité, nous nous substituons à vous » ? Ne serait-ce pas plus intelligent de dire : « dès l'instant que votre enfant est venu au monde, c'est *vous* qui êtes la première en charge de son avenir et de sa protection » ? Est-ce donc une si bonne idée de succomber à une sorte de fascination de la technologie moderne et de se dire que, puisque telle technologie est disponible, il faut automatiquement qu'elle se substitue à l'action humaine ? Il me semble que non… On peut enfin ajouter un dernier argument, qui est sans doute le plus important. Chez le bébé, la conscience et l'autonomie vont *croissant* : il va devenir un enfant, un adolescent, puis un adulte. A un moment dans ce parcours, il va bien falloir accepter de relâcher la surveillance et lui donner son autonomie. Il ne faut donc peut-être pas tout de suite se précipiter sur des technologies qui permettent de le tenir sous contrôle car va se poser ensuite, à un moment donné, une question redoutable: à partir de quel moment va-t-on considérer que la personne peut échapper au système de contrôle ?

Mais, si nous prenons la même technologie, appliquée, cette fois, à des personnes atteintes de la maladie d'Alzheimer, les circonstances sont tout à fait différentes. Tout d'abord, dans ces cas, la conscience et l'autonomie, hélas, vont *décroissant* : les malades d'Alzheimer ont peu d'espoir, en général, de retrouver une conscience plus grande à mesure que le temps passe. Donc, en termes d'intrusivité par rapport à la vie privée, l'enjeu est beaucoup moins lourd que par rapport aux nourrissons. En outre, un malade

d'Alzheimer va pouvoir justement *retrouver une certaine autonomie*, dans un territoire déterminé car, grâce au port d'un bracelet ou d'une puce électronique, il va pouvoir se déplacer plus facilement dans une enceinte parce qu'il sait qu'on pourra le retrouver facilement. Là où on ne peut certainement pas dire que, chez le nourrisson, le port d'un bracelet accroît en quoi ce soit ses possibilités d'autonomie. On voit donc qu'il faut, une fois de plus, examiner chaque cas dans le détail et que l'analyse coûts/avantages ne donne pas toujours le même résultat. Il faut que la CNIL ait le courage de dire à chaque fois : nous pensons que c'est une bonne chose dans tel cas et non dans tel autre.

Je citerai un dernier exemple pour montrer cette fois l'inanité de certains usages dans certaines situations. Il concerne le fait d'utiliser la technologie des puces RFID par injection dans le bras pour les personnes qui souhaitent entrer dans des boîtes de nuit dites « ultra-branchées ». Ce système existe à Mexico, Rotterdam, Madrid et Barcelone actuellement. Les « jeunes branchés » acceptent de se faire injecter dans le bras une puce de la taille d'un grain de riz, dans des conditions sanitaires souvent problématiques, pour un bénéfice aussi dérisoire que de pouvoir entrer, à l'écart des autres, de manière privilégiée. Ils passent leur bras devant un rayon vert qui leur ouvre la porte de la boîte de nuit et défalque automatiquement de leur compte le coût de l'entrée ; de même, chaque fois qu'ils commandent une nouvelle bouteille, le système permet de défalquer son prix de leur compte. Voilà l'exemple type de l'utilisation imbécile d'une technologie. Il est difficile de comprendre qu'une personne raisonnable puisse accepter une telle atteinte à son intégrité physique et mentale pour un bénéfice aussi ridicule. Il convient d'autant plus de lutter contre ce type d'usages qu'ils peuvent avoir un effet dévastateur

sur le plan social par « contamination ». Car, comme on l'a vu, ce type de technologies peut aussi présenter des usages bénéfiques et il ne faudrait pas que ce type d'usages en gâche l'image dans la société.

D. Le « réseau internet »

Je ne m'attarderai pas sur le fonctionnement de cette technologie tant il est bien connu. J'insisterai davantage sur un fait qui, lui, est trop souvent méconnu : il existe, derrière cette technologie, une forme de prosélytisme face auquel il convient de sérieusement s'interroger. Je parle ici des « réflexions » développées notamment par trois des grands patrons du secteur dans différents « écrits ».

Commençons par Mark Zuckerberg, le patron de *Facebook* : garçon extrêmement intelligent, à la tête, à 27 ans, d'un empire planétaire et d'une fortune considérable. Malheureusement, sur le plan « philosophique » des enjeux de son action, sa réflexion n'est pas vraiment à la hauteur. Selon lui, par exemple, la norme sociale a désormais évolué : c'est celui qui ne se montrera pas dans sa nudité – au sens figuré comme au sens propre – sur le réseau qui devra être considéré comme « anormal ». Il faudrait désormais tout dire et tout exposer de soi parce que la norme sociale ne serait plus la même. Beaucoup de jeunes, qui n'ont guère plus de réflexion sur le sujet, le suivent et considèrent comme étant normal un tel phénomène. Ils trouvent « fun » de s'exposer ainsi totalement sur la toile et lorsqu'on leur fait remarquer qu'ils laissent ainsi des informations sur eux, ça et là, leur argument est toujours le même argument que je craignais plus que tout autre président de la CNIL : celui du « *rien à se reprocher, rien à cacher* » [3]. Ce raisonnement absurde et pernicieux confond systématiquement deux notions qui n'ont guère de rapports entre elles : la notion

d'*intimité* et celle d'*innocence*. En réalité, je dois protéger mon intimité quelle qu'elle soit, avec qui que ce soit, que je sois 'innocent' ou 'coupable'! J'ai entendu, à plusieurs reprises, le discours suivant : « si je suis avec ma femme, on peut tout savoir de moi, cela ne me pose pas de problème ; si je suis avec ma maîtresse, par contre, je revendique la protection de ma vie privée ». C'est absurde : il faut revendiquer cette protection dans tous les cas, avec sa femme comme avec sa maîtresse ! On ne voit pas d'ailleurs pourquoi sa femme n'aurait pas autant droit à la protection de son intimité que sa maîtresse… Pour le reste, c'est une question d'innocence et de morale, si l'on y tient, mais il faut bien distinguer entre intimité et innocence.

Deuxième personnage : Eric Schmidt, ancien Président de Google, qui explique tranquillement que le réseau ne peut garantir la possibilité que vous récupériez la totalité de vos données personnelles une fois que vous y êtes entrés. Le modèle économique sur lequel repose le réseau, selon lui, ne le permet pas… Argument stupéfiant : une société privée vient donc expliquer que le modèle économique sur lequel elle est fondée ne lui permet pas de mettre en place les techniques qui feraient que les particuliers – des consommateurs, ou même, disons le mot, des clients - qui lui ont confié des données personnelles puissent les retirer et que, en conséquence, elle se donne le droit de les conserver. Ce discours, on ne l'accepterait d'aucune autre société privée mais, quand Google affirme cela, de manière un peu gênée, des millions de personnes l'acceptent

3. Eric Schmidt argumente exactement de la même manière. Dans un entretien sur CNBC, il estimait par exemple que seules les personnes qui ont des choses à se reprocher se souciaient de la protection de leurs données personnelles.

comme une fatalité.

Mais Eric Schmidt va beaucoup plus loin… Selon lui, sur les réseaux on ne peut préserver son identité, statistiquement qu'environ 7 ans. Il propose ainsi de développer le concept de « séquences d'identité » : il faudrait admettre que, sur les réseaux on peut préserver son identité, statistiquement, environ 7 ans. Au bout de cette période, il faudrait pouvoir reconstruire son identité et donc demander à en changer. Je me suis ainsi retrouvé, il y a trois ans, lors de la conférence mondiale annuelle 'Informatique et Libertés' à Jérusalem, face à deux professeurs de droit de l'Université de Washington qui travaillent, à la demande de Google, sur le concept de « banqueroute de réputation » ou de « banqueroute d'identité ». Au bout de 6-7 ans, un citoyen pourrait faire constater que son identité sur le web est tellement mise à mal et décomposée qu'il se déclarerait en « banqueroute » ; il demanderait alors à l'État de bien vouloir lui reconstituer une identité, c'est-à-dire de changer d'état civil ! Schmidt propose ainsi qu'on puisse changer d'identité tous les 7-8 ans de sorte qu'on aurait 4 ou 5 identités différentes au cours d'une vie d'adulte...

Troisième personnage : Larry Page, co-fondateur de Google et actuellement son Président. Selon lui, Google, à terme, doit devenir une sorte d'institution ou d'être moral universel qui a pour vocation de réunir et de gérer la totalité de la connaissance du monde accumulée. Un jour viendra, selon lui, où les États devront se tourner vers Google… Celui-ci disposant de la totalité des informations sur les citoyens du monde, les États, avec leurs fichiers régaliens classiques, seront relativement bien plus ignorants et devront se tourner vers Google qui décidera de leur transmettre (ou non) telle ou telle information sur leurs citoyens.

Si l'on conjugue les écrits de ces trois personnages, on a de quoi s'inquiéter quelque peu. Or il faut bien constater qu'aujourd'hui bien peu se soucient de ces questions. On a beau l'expliquer et le réexpliquer, cela ne change rien à la façon dont la collectivité envisage son rapport avec ces technologies du numérique.

2. LES RISQUES DES TECHNOLOGIES DU NUMÉRIQUE

On en relèvera quatre.

A. Concentration et synergie des dispositifs

Prenons là encore un exemple concret : il existe actuellement beaucoup de problèmes de hooliganisme dans les stades de football. La ligue de football et le ministère de l'Intérieur ont donc demandé à la CNIL de travailler ensemble sur un projet visant à juguler ces phénomènes. Il a été proposé de mettre en place des systèmes vidéo qui balaieront les tribunes à longueur de match, systèmes qui seront couplés avec un système de reconnaissance faciale biométrique. On intègre donc dans l'ordinateur du système vidéo des centaines de photos numérisées de personnes déjà répertoriées par les services de police comme ayant participé à des émeutes dans les stades. Chaque fois que la caméra passe sur l'un de ces visages, elle marque ce qu'on appelle un « choc » et repère qu'untel était installé à la place X ou Y. On ajoute à cela une puce RFID intégrée dans le billet de stade, qu'il faudra présenter à l'entrée et à la sortie du stade et qui permettra, elle, d'assurer la géo-localisation. Donc : on repère par la photo, on situe grâce à la vidéo et on suit la personne dans ses déplacements grâce au

système RFID. Système remarquable, assurément, mais la question qu'il faut se poser est la suivante : se rend-on bien compte que si on commence à le mettre en place dans les stades, on le fera ensuite dans les aéroports, dans les zéniths, dans les facs, et finalement partout où il y a des lieux de rassemblement public ? A-t-on bien réfléchi au mode de vie que cela implique ? Je ne dis pas que ce soit bien ou mal, je me demande juste si on en a bien pesé toutes les conséquences.

B. La dissémination

C'est le problème du « nuage numérique » : le fait qu'aujourd'hui des milliers d'entrepôts ou de « fermes numériques » élèvent en batterie non pas des poulets mais des disques durs par centaines de milliers, qui traitent à longueur de journées des informations par milliards. Ces systèmes présentent pour les sociétés un grand intérêt car elles peuvent ainsi externaliser la gestion de leurs systèmes de données. Mais mêmes les patrons des entreprises chargées de cette gestion reconnaissent que ces données atteignent de telles proportions qu'elles en finissent par être difficilement contrôlables : ce sont donc des milliards et des milliards de données qui vont tourner pendant des années, dispersées dans le monde entier et qui finiront par devenir comme ce que les juristes appellent des « *res nullius* », n'appartenant plus à personne et sans aucune protection juridique. Ce seront, en quelque sorte, des déchets « infoactifs »… Tandis que, d'un autre côté, ces données existeront toujours et pourront toujours être réintégrées dans le circuit, d'où toute la question fondamentale du droit à l'oubli.

C. La miniaturisation

Nous pourrons, avant 2020, utiliser les nanotechnologies

pour mettre en place des systèmes d'information qui verront, entendront, communiqueront à distance et seront d'une taille telle qu'on ne les verra plus à l'œil nu. La question, une fois de plus, n'est pas de mettre en doute l'utilité incontestable des nanotechnologies, par exemple dans le domaine médical. Il s'agit plutôt de se demander si les pouvoirs publics des États qui accèdent aux nanotechnologies ont engagé une véritable réflexion de fond sur les dangers de ces technologies en matière de systèmes d'information ? La réponse est non, si on laisse de côté quelques initiatives en Espagne, en Allemagne et en France. On avance donc tête baissée, dans ce domaine, en ce qui concerne l'utilisation de ces technologies. Or il faut bien comprendre que, le jour où nous aurons des millions de puces RFID confectionnées à partir d'éléments nanotechnologiques, issues du secteur privé comme du secteur public et dispersées dans la nature, on ne pourra plus les récupérer ni les contrôler. Les citoyens ne sauront ni où elles sont, ni s'ils en sont porteurs. Il y a là un danger grave qui pourrait nous faire regretter le temps du *Big Brother* d'Orwell parce que *Big Brother*, c'est au fond le gros personnage, bien identifiable, qui pense surveiller la société tout entière, tandis qu'il reste malgré tout à celle-ci le droit à l'insurrection ? En revanche, contre des milliers de puces dispersées dans la nature qui nous verront, entendront et enregistreront à notre insu, comment se rebeller ? Contre qui ? Contre quoi ? Et comment les « rappeler » ? Il n'y a actuellement aucune réflexion dans notre société sur ce thème.

D. La dématérialisation

On pourrait presque parler d'informatique « à l'état gazeux ».

L'informatique devient littéralement *dématérialisée*, invisible et ubiquitaire, contextuelle, répandue dans l'atmosphère un peu comme un gaz. Nous allons vivre de plus en plus dans une société où l'ensemble de nos comportements seront vus et analysés à chaque instant. Il est, par exemple, aujourd'hui possible – et la grande distribution y réfléchit – de mettre en place des capteurs capables d'analyser le faciès des personnes, les réactions de leur visage face à un produit pour en déduire une appétence ou un rejet. Des ingénieurs travaillent sur les odeurs dégagées par les personnes pour déterminer si elles éprouvent de la peur, du dégoût, de la joie ou de l'excitation devant tel produit ou tel événement. On va donc vivre de plus en plus dans une société où l'on sera environné de multiples capteurs et de multiples systèmes informatiques dont on ne saura plus trop qui les pilote exactement.

3. LES SOLUTIONS

Trois solutions me semblent possibles.

Tout d'abord, la solution **technologique**, ce qu'on appelle la *privacy by design*, c'est-à-dire le fait d'intégrer dès le début d'un processus technologique le système qui permet d'en juguler les effets néfastes. Tous les experts affirment que beaucoup pourrait être fait en ce sens. On pourrait par exemple faire en sorte que toute donnée qui entre sur le réseau internet intègre en elle-même la date de sa propre disparition. On réglerait ainsi 99% des problèmes de mémoire et donc de droit à l'oubli. Ce serait tout à fait faisable, mais à un coût très élevé et ceux qui pourraient le financer n'ont guère intérêt à le faire.

Deuxième solution, la solution **pédagogique**. C'est là une solution qui, de toute façon, mérite d'être développée. Elle est loin d'être parfaite, son efficacité reste limitée, mais tout ce qu'on peut faire en ce domaine est bon à prendre. Il s'agirait d'engager un important travail auprès du ministère de l'Éducation pour développer des actions à destination des jeunes afin de les aider à vivre leur vie numérique en préservant l'essentiel, c'est-à-dire la jouissance de leurs libertés d'expression et d'aller et venir. Ne nous trompons pas d'enjeu : il ne sert absolument à rien de faire une pédagogie de la *technique*. Les élèves sur ce point sont souvent bien plus avancés que les maîtres. Le rôle du professeur serait plutôt de rappeler ce que sont les notions fondamentales de libre arbitre, d'intimité et d'identité, c'est-à-dire de doter le jeune élève d'une certaine *conscience* par rapport à ces phénomènes technologiques afin qu'il puisse les appréhender en adulte. Il me ne semble pas, hélas, que le ministère de l'Éducation ait encore bien compris les enjeux d'une telle action. Espérons que les choses avancent sur ce point.

La troisième solution serait la solution rêvée mais c'est assurément la plus difficile à atteindre et je ne nourris plus guère d'illusions, à moyen terme, sur ce point. Il s'agit de la solution *juridique*. Elle suppose de convaincre d'abord les autres pays européens qu'il faut se retourner ensemble vers les États-Unis et essayer de combler ainsi le fossé considérable, quant aux conceptions défendues, qui sépare les deux côtés de l'Atlantique. Puis il faudrait ensuite se tourner tous ensemble vers l'Asie et essayer de mettre en place un système juridique commun pour assurer une régulation, via une convention internationale à contrainte juridique sous l'égide de l'ONU. Mais pour cela, il faudrait déjà qu'à Bruxelles des décisions lourdes soient prises dans

le cadre du projet de règlement sur lequel on travaille actuellement. Il faut espérer que se dégage une position européenne globale face aux États-Unis. Ce qui me semble préoccupant, c'est que le processus conduisant à une telle convention sera de toute façon long et tortueux : pendant ce temps, tous les dangers que j'ai évoqués seront devenus des réalités et il sera un peu tard pour agir à leur égard.

CONCLUSION

Une prise de conscience est nécessaire. Certains signes laissent espérer qu'elle commence à poindre : j'avais ainsi demandé à l'équipe du Président de la République s'il était possible d'inscrire quelques lignes sur ce sujet dans le communiqué final du G8 sur le numérique et cela a été fait. C'est déjà une avancée. Mais je sais aussi que les Américains se sont fermement opposés à tout effort pour aller plus loin… Il me semble que nous nous trouvons actuellement dans une situation comparable à celle où nous étions en 1974 lorsque René Dumont est venu présenter ses thèses écologiques lors de la campagne présidentielle. Il déclarait alors que, si on n'y prenait garde, dans trente ans, le climat sera tellement détraqué qu'on ne pourrait plus rien faire. On l'a pris alors pour un hurluberlu… Trente cinq ans après, les experts nous disent qu'il est peut-être maintenant trop tard pour intervenir. On peut en déduire qu'à un moment donné, cette intervention était encore possible ! C'est exactement à ce moment que nous sommes en ce qui concerne les technologies du numérique et la protection de la vie privée : c'est *maintenant* qu'une prise de conscience est nécessaire afin pouvoir

utiliser ces technologies du numérique dans un cadre véritablement régulé et contrôlé par le corps social. Et, pour cela, il faut commencer par expliquer à nos concitoyens que, de la même manière que nous sommes en charge de notre environnement collectif (l'environnement naturel), nous sommes aussi en charge de notre environnement *individuel*. Au sein de cet environnement, il y a ce que les anglo-américains appellent notre *privacy*, cette sorte de sphère dans laquelle on trouve la protection de la vie privée, de l'intimité et de l'identité. C'est un patrimoine qui nous est donné à la naissance et que nous devons protéger coûte que coûte. Il y a là, on le voit, une réflexion à mener, comparable à celle qui a eu lieu pour la protection de l'environnement naturel, et nous devrions nous servir du retard pris dans ce dernier cas pour éviter de prendre le même retard une nouvelle fois.

Retrouvez l'intégralité du débat en vidéo sur www.institutdiderot.fr

Les publications de l'Institut Diderot

Dans la même collection

L'avenir de l'automobile
Louis Schweitzer

Les nanotechnologies & l'avenir de l'homme
Etienne Klein

L'avenir de la croissance
Bernard Stiegler

L'avenir de la régénération cérébrale
Alain Prochiantz

L'avenir de l'Europe
Franck Debié

L'avenir de la cybersécurité
Nicolas Arpagian

L'avenir de la population française
François Héran

L'avenir de la cancérologie
François Goldwasser

L'avenir de la prédiction
Henri Atlan

L'avenir de l'aménagement des territoires
Jérôme Monod

L'avenir de la démocratie
Dominique Schnapper

L'avenir du capitalisme
Bernard Maris

L'avenir de la dépendance
Florence Lustman

L'avenir de l'alimentation
Marion Guillou

L'avenir des humanités
Jean-François Pradeau

L'avenir des villes
Thierry Paquot

L'avenir du droit international
Monique Chemillier-Gendreau

L'avenir de la famille
Boris Cyrulnik

L'avenir du populisme
Dominique Reynié

L'avenir de la puissance chinoise
Jean-Luc Domenach

L'avenir de l'économie sociale
Jean-Claude Seys

Les Notes de l'Institut Diderot

L'euthanasie, à travers le cas de Vincent Humbert
Emmanuel Halais

Le futur de la procréation
Pascal Nouvel

La République à l'épreuve du communautarisme
Eric Keslassy

Proposition pour la Chine
Pierre-Louis Ménard

L'habitat en utopie
Thierry Paquot

Les Dîners de l'Institut Diderot

La Prospective, de demain à aujourd'hui
Nathalie Kosciusko-Morizet

Politique de santé : répondre aux défis de demain
Claude Evin

La réforme de la santé aux Etats-Unis : quels enseignements pour l'assurance maladie française ?
Victor Rodwin

Les Entretiens de l'Institut Diderot

L'avenir du progrès (actes des Entretiens 2011)

L'avenir de la vie privée dans la société numérique

Voici un appel à la réflexion et à l'action face au « déferlement numérique » auquel nous assistons trop passivement. Cet appel émane de celui qui de 2004 à 2011 a présidé la Commission nationale de l'informatique et des libertés (CNIL).

Il s'appuie sur des exemples concrets empruntés à ces grands domaines que sont la vidéosurveillance, la biométrie, la géo-localisation et le réseau informatique mondial.

La vie privée et l'intimité des citoyens se trouvent indéniablement menacées ; la majorité des internautes n'a pas conscience de l'utilisation possible, grâce à l'évolution extrêmement rapide des technologies, de ses données personnelles par les grands acteurs de l'Internet ou par un gouvernement. Mais Alex Türk n'est pas un penseur catastrophiste. Il ne dénigre pas les technologies nouvelles ou l'intelligence créative des grands noms du web. Aucune fin du monde n'est annoncée. En revanche, l'ancien président de la CNIL avance des solutions pour mieux protéger la liberté des citoyens. On ne s'étonnera pas que ces solutions reposent en définitive sur la prise de conscience et la mobilisation de tous.

Pr. Dominique Lecourt
Directeur général de l'Institut Diderot

Alex Türk

Alex Türk est Sénateur du Nord (Nord-Pas-de-Calais). Ancien Président de la Commission nationale de l'informatique et des libertés (CNIL) de 2004 à 2011, Président de l'Autorité de contrôle de Schengen de 1995 à 1997, Président de l'Autorité de contrôle commune des fichiers de l'European Police Office (Europol) de 2000 à 2002 et président d'EURODAC.

INSTITUT DIDEROT

FONDS DE DOTATION POUR LE DEVELOPPEMENT DE L'ECONOMIE SOCIALE REGI PAR LA LOI N°2008-776 DU 4 AOUT 2008 - SIRET N° 513 746 651 00019
11, place des 5 martyrs du lycée Buffon 75014 Paris / T. +33 (0)1 53 10 65 60 / F. +33 (0)1 53 10 65 36
contact@institutdiderot.fr / www.institutdiderot.fr

Conception 4uatre.fr - Réalisation www.idcomm.fr - Imprimé sur papier issu de forêts gérées durablement.