Notre identité numérique en 2025 ?

Michel Arnaud

Notre identité numérique en 2025 ?

Michel Arnaud
Université Paris Ouest Nanterre la Défense

Faire de la prospective est hasardeux car il est difficile de prévoir ce qu'il va se passer. Toutefois les tendances actuelles concernant les usages des réseaux se dessinent avec suffisamment de netteté pour pouvoir être extrapolées dans un délai de 15 ans sous forme de scénarios plausibles. Essayons ensemble de faire une projection sur ce qui pourrait se produire.

Serons-nous habitués à être branchés en permanence sur les réseaux au point de ne pas pouvoir nous déconnecter ? Étant donné, d'une part, l'effort des administrations et des fournisseurs privés pour mettre en ligne leurs services et, d'autre part, le degré d'immédiateté auquel nous habituent les échanges sur les réseaux sociaux, la déconnexion devient de moins en moins envisageable car elle se ferait au détriment de notre bien-être et peut-être de notre sécurité. Dans le cas de malades devant être surveillés en permanence, les alertes ne pourraient pas être activées en réaction aux informations transmises à partir des capteurs répartis sur leur corps. Les personnes qui malgré tout préféreraient se déconnecter des réseaux pour conserver leur liberté de manœuvre, le feront à leurs risques et périls. A notre sens il y en aura de moins en moins.

La nécessité d'être constamment relié aux services de contrôle en ligne pour réduire les risques, et la volonté de ne plus avoir à se soucier des outils de communication que nous risquons toujours de perdre favoriseront le mode des implants sous la peau. Comment, avec un tel dispositif, pourrons-nous accéder nous-mêmes aux informations si les implants communiquent directement avec les systèmes de contrôle en ligne ? Le terminal intelligent implanté sous la peau pourra dialoguer avec un clavier de format interchangeable et adaptable à tous les types d'écriture. De même toutes sortes d'écrans en 3D seront utilisables pour projeter les images et faciliter la transition entre mondes réel et virtuel.

Le cœur des informations personnelles, à savoir les identifiants biométriques, sera stocké dans l'implant sous la peau. Ce sera une manière d'arrimer dans son corps un coffre-fort électronique dans lequel se trouveront les preuves intangibles de son identité biométrique. Dans une telle société, la transparence sera la meilleure défense contre la fraude : celles et ceux qui n'auront rien à cacher seront les plus à même de démontrer leur bonne foi s'il advenait qu'ils soient à tort soupçonnés d'actions répréhensibles à cause d'une usurpation d'identité. Démontrer qui on est ne prendra qu'une fraction de seconde, le temps de faire vérifier son identité biométrique par les contrôleurs des réseaux. Pour tout achat, un certificat électronique basé sur la biométrie pourra par exemple être produit, manière de lutter efficacement contre le vol d'identité.

Toute la question est le degré de liberté individuelle laissé dans un tel système à chaque citoyen. Est-ce que l'on va s'habituer à faire systématiquement appel aux contrôleurs des réseaux, à savoir la police, la justice, le fisc, pour assurer notre sécurité ? Autrement dit, est-ce que le dévoilement de son identité biométrique va devenir un sésame tellement courant qu'on n'y prêtera plus attention ?

Utiliser un pseudo a mauvaise presse : se cacher est lié à l'idée d'une action répréhensible qu'on veut pouvoir dénier. Pourtant le pseudo comme l'anonymat sont utiles pour ne pas être tracé en tant que personne identifiée. Donner la possibilité d'utiliser un pseudo ou d'agir anonymement équivaut à laisser des zones de semi-liberté où le citoyen peut se mouvoir sans être reconnu, tant qu'il n'est pas soupçonné de mauvaise action. Dans le cas contraire, son pseudo ou son anonymat sera cassé et le lien avec sa véritable identité rétabli par les pouvoirs publics.

C'est bien vers ce type de société que nous nous engageons à grands pas. Si la démocratie est garantie par l'équilibre entre les trois pouvoirs, il reste à voir comment la législation donnera au citoyen un droit de contrôle sur la divulgation de son identité, en dehors des situations d'urgence où son intégrité physique ou celle des autres seront menacées.

On peut objecter que ces plages de semi-liberté ne sont que des pis aller par rapport à la liberté fondamentale, mise à mal par la connexion de tout un chacun aux réseaux. Mais la vie quotidienne s'en trouvera allégée si chacun peut jouer sur plusieurs registres d'identité. Un système d'identités multiples sera disponible sous forme de gestion de ses attributs certifiés (solvabilité, âge, etc.) à associer avec des services particuliers sans pour autant devoir révéler sa véritable identité biométrique aux fournisseurs.

Le tiers de confiance sera l'organisme qui gèrera la relation entre le client et le fournisseur de services. Il aura accès aux données personnelles biométriques de chacun stockées dans son implant, parce que ce dernier l'aura autorisé à le faire, à l'inverse de la police, de la justice et du fisc qui auront accès de plein droit à ces informations. Le tiers de confiance aura obligation de ne pas révéler les données personnelles du client aux fournisseurs de services. Par contre, il pourra certifier auprès des fournisseurs que le client est solvable, qu'il a droit à tel tarif lié à son âge, etc.

Toutes les données relatives à nos comportements seront stockées dans des fermes de serveurs fonctionnant en nuages, c'est-à-dire sans qu’on puisse localiser exactement où elles seront réellement entreposées. Mais qui s'en souciera ? Les dispositifs juridiques auront réussi à imposer une différenciation entre données personnelles et données relatives à nos habitudes d'achat. Depuis son enfance, le citoyen sera habitué à dialoguer avec les tiers de confiance dans des boutiques de proximité réelles ou virtuelles. La protection des données personnelle par conception (privacy by design) aura cessé d'être un slogan pour devenir une réalité.

Le débat démocratique portera sur la nature du tiers de confiance : soit un acteur monopolistique comme nous les connaissons à présent, avec les risques de prise de contrôle des échanges économiques, soit un acteur proche du client au sens où il pourra le rencontrer dans sa boutique réelle ou virtuelle, médiateur humain tel un notaire gardien de l'identité sur les réseaux. L'humanisation des relations sur les réseaux sera au centre des débats politiques dans les années à venir, au sens où la question portera sur les meilleures manières d'impliquer le citoyen dans la société en réseaux tout en préservant au mieux son libre arbitre.

Ce débat n’est pas vain au moment où l'identité biométrique risque de devenir le marqueur de la traçabilité permanente. Le réchauffement climatique pourrait notamment justifier l’adoption de mesures drastiques de la production de CO_2, avec comme conséquence un contrôle étroit des déplacements. Le rôle des tiers de confiance serait dans ce cas un enjeu de liberté citoyenne, en tant que rempart de la liberté de choix et de comportement contre le contrôle étatique généralisé.