

Avant-propos

Usurpations d'identités en grand nombre, violations répétées de la vie privée des individus, constitution de bases de données gigantesques, fichage généralisé... Quelque chose ne va pas dans le monde d'Internet et des réseaux. Au centre de ce maelström, l'identité numérique.

La première raison à cette situation tient à ce que l'identité sur le « réseau des réseaux » a été à l'origine délaissée par les pionniers d'Internet.

À la différence d'Internet, bien des réseaux informatiques ont été conçus de telle façon que l'identité de l'accédant soit vérifiée à l'entrée du réseau. Par exemple, le réseau informatique des cartes bancaires permet, partout dans le monde, en tout temps et à toute heure, de procéder à des retraits d'argent en espèces. Ce réseau est réservé à un public qui s'authentifie préalablement et obligatoirement au double moyen d'une carte délivrée par une banque et de la saisie d'un code confidentiel personnel. Sauf fraude, l'anonymat n'y a pas sa place.

Internet, quant à lui, ne se préoccupe pas d'identifier ses utilisateurs, même si ces derniers y accèdent majoritairement *via* des fournisseurs d'accès qui les ont identifiés. Il existe de nombreuses façons d'échapper à cette identification (accès publics, « anonymiseurs », etc.).

À l'inverse, face à ce vide, certains opérateurs organisent des communautés d'utilisateurs prédéterminés et sélectionnés, dont ils exigent l'identification préalable. Le professeur de droit Lawrence Lessig¹ a décrit

1. Lawrence LESSIG, *Code and Other Laws of Cyberspace*, Boston, Basic Books, 1999.

comment son université, à Boston, l'un des premiers centres d'éducation et de recherche dans le domaine du droit, réservait l'accès à Internet à des machines préalablement autorisées et vérifiées. Dans ces conditions, sauf à usurper une identité ou à pirater une machine, la personne connectée est immédiatement identifiée, sans possibilité d'anonymat. Une telle organisation n'est toutefois possible que lorsque la communauté est peu importante et que des ressources (contrôle par un opérateur humain, moyens techniques) existent pour gérer les identifications préalables.

Pourquoi la question de l'identité a-t-elle été délaissée par les pionniers d'Internet ? Selon certains, ses fondateurs ont pris le parti de favoriser l'anonymat parce qu'ils estimaient qu'il pouvait à la fois garantir la liberté d'expression et assurer le principe d'égalité des internautes. D'autres avancent l'hypothèse que ces pionniers souhaitaient laisser à chacun le choix de son identité en n'imposant pas un système d'identité unique. Enfin, et plus simplement, il est possible que les pionniers aient privilégié la simplicité d'accès au réseau, qui est d'ailleurs à la base de son succès, en excluant toute identification préalable obligatoire.

Quoi qu'il en soit, l'absence de traitement de l'identité a ouvert des brèches qui ont conduit à la situation actuelle, où la défense de l'identité numérique est devenue un problème.

En entreprise, l'identité numérique est aussi omniprésente. Tout nouveau venu se voit attribuer de manière quasi systématique des identifiants et mots de passe pour accéder à son ordinateur et à l'intranet de l'entreprise. Il dispose en outre d'une adresse e-mail pour échanger avec ses collègues, les clients, les fournisseurs.

Les problèmes soulevés par l'identité numérique semblent moins criants dans ce contexte. L'employeur, dans le cadre de son pouvoir de direction, sait normaliser les relations au sein de l'entreprise. Chartes d'usage Internet, contrats de travail, notes de service, cybersurveillance se multiplient pour gérer au mieux les identités numériques. Des normes juridiques et pratiques voient le jour, dont la loi et les tribunaux sanctionnent les abus, notamment les atteintes à la vie privée sur le lieu de travail. Mais salariés et employeurs ne savent pas toujours où se situent les limites juridiques de ces nouveaux usages et leurs responsabilités.

Les questions soulevées par l'identité en général sont aussi anciennes que la société des hommes, et l'on peine toujours à en donner une définition unanime. De la philosophie aux sciences sociales en passant par les sciences naturelles, chacun fournit la sienne.

Notre propos n'est pas d'en dresser l'inventaire ni de proposer une définition théorique de l'identité à l'heure numérique. Nous nous bornerons à établir des constats du point de vue juridique :

- Aux côtés des fondements génétiques, biologiques, psychologiques, sociologiques et culturels de l'identité, s'en ajoute un nouveau : le contexte numérique. Ce contexte a généré une nouvelle identité, que nous appelons « identité numérique ».
- L'identité numérique est partout présente dans l'espace public qu'est Internet comme dans l'entreprise, mais cette présence n'est pas « normée » de manière satisfaisante. Elle s'affirme au travers d'une multitude d'identifiants numériques non ou mal gérés.
- L'identité numérique est probablement l'une des clefs de compréhension de la société de l'information dans laquelle nous sommes entrés, et elle dépasse largement la seule question identitaire. La difficulté, voire l'impossibilité d'identifier les internautes explique, par exemple, pourquoi les pouvoirs publics peinent tant à lutter contre la contrefaçon, en dépit d'un train de mesures répressives qui se multiplient d'année en année.

Organisation de l'ouvrage

Par cet ouvrage, nous souhaitons engager une réflexion juridique ouverte et accessible à tous sur l'identité numérique. La problématique de l'identité numérique mêle des questions techniques, juridiques et organisationnelles. Ces questions recèlent des enjeux fondamentaux pour le devenir de la société de l'information.

Pour aider le lecteur à comprendre ces questions et ces enjeux, nous avons organisé l'ouvrage en onze chapitres.

- Le chapitre I commence par introduire les problématiques juridiques générales posées par les identifiants numériques. Ces identifiants sont indispensables à la construction d'une identité numérique.

- Le chapitre II soulève la question de l'anonymat sur les réseaux et de son traitement par la loi : est-il légal, et si oui dans quelles limites ?
- Le chapitre III se penche sur les traces. Pour contrer l'anonymat, le législateur a rendu la collecte des traces obligatoire. Nous verrons quels sont les contours exacts de cette obligation de traçage et constaterons qu'elle vise bien plus que les seuls fournisseurs d'accès Internet.
- Les chapitres IV à VI détaillent ces identifiants numériques omniprésents que sont le pseudo, le nom de domaine et le mot de passe et les abordent au travers des difficultés juridiques spécifiques qu'ils soulèvent.
- Les chapitres VII et VIII portent sur les titres et les registres d'identité. Tout système d'identité, qu'il soit numérique ou non, délivre des titres d'identité, comme la carte nationale d'identité, et gère un registre d'identité, comme le registre de l'état civil. Mais comment peuvent s'envisager des titres et des registres dans un système d'identité numérique ?
- Les chapitres IX à XI se penchent sur trois symptômes propres à Internet, conséquences de l'absence d'un système d'identité numérique global : la lutte pour la défense du droit à l'image et contre les nouvelles formes d'usurpation d'identité, notamment le « phishing », ainsi que la difficulté d'échapper à son identité numérique du fait de l'omniprésence des moteurs de recherche qui collectent et enregistrent tout.

L'identité numérique engendre de multiples problèmes. Si nous sommes encore loin d'avoir apporté toutes les solutions, au moins pouvons-nous nous poser les bonnes questions. Pour cela, une claire vision juridique de ces problèmes est nécessaire. Cet ouvrage ne vise à rien d'autre qu'à apporter cette pierre à l'édifice.