Dans la jungle des identifiants numériques

Serge Abiteboul

Dans la jungle des identifiants numériques

A quoi servent les identifiants numériques ? Comment se retrouver dans la jungle de ces identifiants ? Qu'est-ce qu'impliquent les identifiants uniques privés ou étatiques ? Est-ce que de tels identifiants sont souhaitables ? Nous essayons de répondre à ces questions.

Serge Abiteboul

Une identité nationale avec un adresse physique nous identifie depuis les débuts de l'État civil. Depuis le siècle dernier, d'autres « identités », une adresse courriel ou un numéro de téléphone mobile, nous permettent de recevoir des messages ou des appels où que nous soyons et à n'importe quelle heure. Ce siècle, les réseaux sociaux se sont également emparés du sujet : nous avons des identités sur Facebook, Instagram, WhatsApp, etc., plusieurs si nous le souhaitons. Les identifiants associés nous permettent d'accéder à des données protégées, nous exprimer, acheter, vendre, etc. Ils sont indispensables pour une quantité de services géniaux.

Combien d'identifiants numériques sommes-nous capables de retenir pour tous les services que nous utilisons, surtout si on insiste pour les rendre plus complexes (nombre de caractères minimum, majuscules, chiffres, caractères spéciaux, etc.) ? Pour gérer cette profusion, nous pouvons bien sûr nous équiper d'un gestionnaire de mots de passe totalement sous notre contrôle comme KeePass Password Safe, un logiciel libre. Mais cela reste compliqué et si cela nous permet de nous authentifier dans divers services, cela ne permet pas de nous identifier véritablement, de prouver que nous sommes vraiment nous-même. Nous ignorerons ici les identifications biométriques qui soulèvent d'autres questions.

Nous savons bien ce que nous souhaitons : utiliser le monde numérique en toute sécurité, en protégeant la confidentialité de nos données, avec un minimum d'efforts. Les informaticiens disposent avec la cryptographie, la vérification de protocoles, les preuves *zéro-knowledge*, etc., de toute une batterie de techniques pour nous le permettre. Mais le sujet est complexe, les solutions satisfaisantes sont difficiles à mettre en place, et ce n'est pas simple de les faire émerger quand les entreprises privées et les États impliqués lorgnent dans le même temps sur nos données personnelles.

Nous pourrions peut-être adopter des services d'authentification unique (en anglais, SSO de *single sign-on*) comme c'est déjà souvent le cas dans le monde professionnel. C'est ce que les géants du numérique proposent avec enthousiasme : leurs identifiants comme identités numériques universelles. Avec Facebook Connect, par exemple, nous pouvons déjà utiliser, en plus de tous les services du groupe, ceux de bien d'autres entreprises encore. Ce serait finalement tellement simple de n'avoir à retenir qu'un seul couple (login, mot de passe), le leur, bien sûr.

En quoi est-ce que cela serait dérangeant ? D'abord, parce que ces entreprises qui nous facilitent tellement la vie profitent de l'occasion pour consolider des masses de données sur nous, pour les plus grands risques de violation de notre intimité. Ces identifiants « universels » qu'elles proposent nous enferment dans des écosystèmes, accentuent toujours plus la dissymétrie d'information, cause potentielle de risques immenses, à commencer par la

manipulation de l'opinion publique. Ces monopoles privés cannibalisent les messages que nous postons, nos données de navigation, nos *likes*, nos centres d'intérêt, etc. Ils reconstruisent notre véritable identité numérique. Ils s'approprient numériquement cette identité.

Mais peut-être est-il inévitable dans un monde parfaitement numérique et de plus en plus complexe d'aller vers un identifiant unique ? Absolument pas. Il est tout à fait possible de faire coexister plusieurs systèmes d'identification. Chaque opérateur télécom a le sien et pourtant, on peut téléphoner à n'importe qui. La solution tient dans l'interopérabilité. Des services peuvent collaborer même s'ils ne s'appuient pas sur le même système d'identifiants, par exemple, des banques et des e-commerçants qui utilisent pourtant des systèmes d'identification distincts. La technique informatique permet cette complexité… avec quelques efforts bien sûr.

N'est-il pas préférable d'organiser plutôt une grande dispersion de nos données privées sous différents identifiants, de nous construire un petit espace de liberté en refusant d'utiliser leurs identifiants ailleurs que sur leurs propres services ?

Et puis, le fait même que des entreprises privées proposent une « identité universelle » interpelle. La gestion de l'identité est, en France, une prérogative de l'État depuis le 18e siècle. Avec un territoire, le cyberespace, une population, des centaines de millions d'utilisateurs voire plus, une autorité, des règles qu'elles nous imposent, ces plateformes se rêvent déjà en États. En s'appropriant des prérogatives régaliennes d'identité nationale, elles vont un cran plus loin. Que veulent-elles faire d'une telle autorité ? Qui contrôle ce qu'elles en font ? Surtout, d'où tirent-elles la légitimité de cette autorité de pouvoir décider qui nous sommes, ou pas ?

Si l'identité numérique pose problème dans le privé, va-t-elle de soi dans le public où elle se devrait d'être pierre de voute de la citoyenneté dans un monde devenu numérique ? Non, elle pose également problème. La numérisation de l'État patine alors qu'il n'y a pas de raison essentielle pour qu'il soit plus compliqué d'interagir avec les impôts ou la sécurité sociale qu'avec Google ou Amazon. Mais ne jetons pas la pierre aux différents services. Les entreprises traditionnelles avec souvent d'énormes moyens financiers peinent aussi à réaliser la transition numérique.

Pour déployer des services numériques, les services de l'État ont besoin d'identifier numériquement leurs « utilisateurs », les citoyen·ne·s. Le paysage de l'identité numérique public a été bouleversé dans notre pays par France connect, un service d'identification numérique mis en œuvre par la DINSIC. Ce dispositif est proposé comme un « bien commun mis à la disposition de toutes les autorités administratives ». Un objectif de France connect est (entre autres) de procurer un service d'identification *unique* pour tous les services de l'État. L'identification numérique régalienne est d'ailleurs devenue une sorte de totem avec France connect et plus récemment avec la reconnaissance faciale et Alicem.

Relativisons d'abord le sujet. L'identification numérique est une des facettes de la numérisation de l'État, mais c'est loin d'être la seule. Il en est de plus essentielles comme la lutte contre la fracture numérique ou la nécessité d'interfaces utilisateurs « amicales » (*user friendly*). En particulier, la lutte contre la fracture numérique est un chantier énorme ; il n'est pas acceptable d'oublier la partie conséquente de la population qui n'a pas accès au numérique par manque de connexion, de matériels, ou plus massivement encore, par manque des capacités cognitives pour le faire (l'illettrisme numérique).

Maintenant, demandons-nous si l'objectif d'unicité de France connect est souhaitable. Peut-être, parce qu'une identification unique facilite la tâche de l'État avec la promesse de régler d'un coup, d'un seul, les questions d'identification dans ses différents services. A court terme, l'interconnexion des bases de données de l'État qu'elle autorise apporte beaucoup en termes de simplification des processus. A plus long terme, en permettant la consolidation des données accumulées pour une personne par les différents services de l'État, elle introduit également des risques sur nos vies privées. Toutes ces données dispersées dans les fichiers de l'État recoupées, consolidées, captureraient notre identité, permettraient un contrôle cauchemardesque des citoyens. C'est bien pour cela que la société aura à être particulièrement vigilante sur les utilisations qui seront faites de l'identification numérique publique par l'État.

France connect propose maintenant à des entreprises privées d'adopter son dispositif. Le point particulièrement intéressant est que le système garantit que les informations pour se connecter ne peuvent pas être collectées, échangées, ou vendues. De plus, le système isole le mécanisme d'identification du service spécifique utilisé. Pour illustrer, considérons le visionnage de films pornographiques. Aujourd'hui, pour protéger la confidentialité des adultes, on ne contrôle rien et des enfants sont exposés aux pires contenus. On pourrait exiger une identification avec France connect. Un dialogue entre le site porno et un service d'identité nationale s'établit et permet de garantir que seuls les adultes puissent bénéficier de ce site, sans avoir à divulguer aux services publiques l'activité à laquelle ces adultes se livrent. Cette illustration n'est-elle pas bien triviale pour parler d'un sujet aussi important que l'identité numérique ? Peut-être, mais faire que les enfants soient moins exposés à la pornographie sans enfreindre les libertés de chacun, est-ce finalement un but si trivial ?

Dans nos vies numériques, nous avons de multiples interlocuteurs. Un service d'identification comme France connect doit pouvoir interopérer avec des services publics et privés en limitant l'information échangée au strict minimum. Ces échanges de données doivent être soumis à des lois au-delà du RGPD pour protéger nos données personnelles contre des entreprises ou des États trop curieux. Ce sont les préoccupations qui semblent guider les projets de mise à jour de la régulation eiDAS (Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive) par la Commission Européenne. L'idée serait d'aboutir à une identité européenne qui permettrait de se dégager des identités proposées dans des écosystèmes privés, d'éviter donc de se trouver piégé dans ces systèmes, tout en protégeant nos données personnelles.

Est-ce complètement satisfaisant ? Aujourd'hui non. Ça ne l'est pas d'abord parce que les utilisateurs ont du mal à se repérer dans la jungle de la sécurité et de l'authentification. Il leur faudrait monter en compétence et il faudrait également qu'on leur propose un monde plus simple avec des options claires et compréhensibles par eux. Mais, ne rêvons pas, le sujet restera compliqué et on ne peut s'attendre à ce que l'utilisateur gère seul à la fois ses interactions avec les services du réseau, la confidentialité de ses données, et la sécurité de sa vie numérique. Pour reprendre le contrôle de ses données personnelles, le citoyen et la citoyenne doivent pouvoir s'appuyer sur des systèmes d'information personnelle à leur service qui les aident à contrôler les échanges de leurs données entre les différents services utilisés. De tels systèmes leur sont indispensable pour un jour, pouvoir gérer les embarras d'intendance des connexions aux services privés et public du réseau, et l'impossible (aujourd'hui) question du « consentement » supposé libre et éclairé à ouvrir leurs données personnelles qu'on attend d'eux.