Numérique et confiance

Par **Henri ISAAC**
Université Paris-Dauphine, PSL

Introduction

L'univers numérique s'est développé à une vitesse et une intensité telles que le questionnement de la confiance en cet espace peut paraître incongru. Cependant, dès 2004, la France traduit la directive européenne « E-commerce » en droit français sous le nom « loi pour la confiance dans l'économie numérique » (LCEN), concrétisant l'existence d'enjeux spécifiques de confiance liés à l'espace numérique. Au-delà de la question des transactions marchandes, des enjeux de confiance émergent avec la multiplication des contenus générés par les utilisateurs et, avec ceux-ci, les contenus toxiques (*fake news*). Les comportements des utilisateurs peuvent également amoindrir la confiance en cet espace (fraude en ligne, usurpation d'identité, cyberharcèlement). Par ailleurs, la collecte massive de données personnelles opérée par de nombreux services numériques interpelle. Des risques de nature différente – cybercriminalité, surveillance étatique des communications – entravent également le développement de la confiance en ligne.

Dès lors, un tel espace interroge profondément la question de la confiance ainsi que les mécanismes qui la produisent et l'entretiennent. Univers de confiance pure, l'espace numérique a dû construire de nombreux mécanismes et dispositifs pour créer de la confiance et faciliter le développement des usages. Si ces mécanismes de confiance ont dans un premier temps imité les mécanismes classiques développés dans le monde physique, l'univers numérique a progressivement produit des mécanismes de génération et de gestion de la confiance propres, en s'appuyant sur la nature de ce qui le caractérise, l'organisation réticulaire et le traitement des données.

Dès lors, l'architecture classique du tiers de confiance, quelle qu'en soit sa modalité, pose elle-même question et débouche sur l'idée qu'une architecture de réseau, par conception, par elle-même, peut générer la confiance dans les échanges.

Les multiples défis de la confiance à l'ère numérique

La confiance des individus dans les artefacts technologiques est une problématique ancienne (Taddeo, 2009). Ainsi, la confiance que l'on peut accorder à un robot est une problématique largement étudiée (Coeckelbergh, 2010). Cependant, les enjeux de confiance à l'ère numérique ne se limitent pas à la confiance dans les machines, mais à la confiance envers des dispositifs mêlant des technologies et des comportements humains permis par des infrastructures technologiques distribuées à une échelle mondiale.

L'espace numérique est à la fois un espace informationnel et un espace marchand dans lequel des transactions ont lieu. Dans cet espace, des acteurs malveillants se livrent à de nombreuses attaques, actes de piraterie, et les États eux-mêmes déploient des stratégies de surveillance, qui ont fait l'objet d'un éclairage nouveau après les révélations d'Edward Snowden. Dès lors, la construction de la confiance dans un tel espace fait face à de nombreux défis.

Confiance dans les transactions

Le développement de la sphère marchande sur le *web* a entraîné un questionnement sur la sécurité des transactions dématérialisées. Si cette question a fait l'objet d'une importante réflexion dans

les réseaux professionnels, comme les réseaux utilisant l'EDI [1], force est de constater que la transformation du *web* en espace marchand a rapidement interrogé la confiance que les utilisateurs pouvaient avoir dans les sites et les transactions qui s'y déroulaient. L'impossibilité de déployer des architectures de certificats électroniques auprès du grand public a permis le développement d'une fraude significative dans les transactions en ligne, éloignant pendant de nombreuses années une part substantielle de clients potentiels. Si cette fraude n'a eu de cesse de diminuer depuis une décennie [2], et si 62 % des français effectuent des achats en ligne [3], la question de la sécurité demeure encore un frein au développement des transactions en ligne.

Confiance dans les contenus numériques et l'usage des données collectées

La multiplication des plateformes de médias sociaux a facilité le développement et la propagation de fausses informations. Ces plateformes ont également été utilisées dans de nombreuses campagnes de désinformation initiées par des États. Cette situation conduit les utilisateurs de par le monde à n'accorder qu'une faible confiance à ces espaces informationnels, comparativement à des médias traditionnels. L'étude du Reuters Institute de 2020 met en évidence que 56 % des personnes s'inquiètent de la véracité de l'information publiée sur les réseaux sociaux, cette proportion s'élevant à 84 % au Brésil et 67 % aux États-Unis. Dès lors, seuls 26 % des personnes font confiance aux réseaux sociaux pour s'informer contre 59 % aux médias traditionnels (Reuters Institute, 2020). Mais l'exposition de certains utilisateurs à des contenus dits toxiques (propos haineux, terrorisme, pédopornographie, prostitution) contribue également à amoindrir la confiance que les utilisateurs ont dans les services de réseaux sociaux.

Les services numériques reposent largement sur des traitements de données et particulièrement de données personnelles. Si celles-ci font l'objet d'un cadre juridique renforcé en Europe, force est de constater que certains services en ligne collectent massivement des données personnelles dont la finalité de traitement est opaque et très souvent inconnue des utilisateurs. Les cookies tiers collectés sur des sites éditoriaux à des fins publicitaires sont typiques de ce genre de collecte, qui instille un doute sur la finalité. Ainsi, le questionnement sur les finalités des collectes de données demeure une interrogation très présente pour 76 % des utilisateurs français en 2019 [4]. Cette collecte massive expose également les utilisateurs à un risque de fuite de leurs données par manque de protection et de sécurité du stockage de leurs données. Ces fuites de données sont une réalité qui concerne tout type d'acteurs [5], et elles ont tendance à se multiplier.

Surveillance, cybersécurité et confiance en ligne

La migration progressive et constante des interactions marchandes et non marchandes sur les plateformes numériques conduit plusieurs auteurs à considérer que ces plateformes exercent *de facto* une surveillance de nos comportements et de nos actions. Les plateformes auraient la capacité de manipuler les choix de contenus et par la même nos décisions et comportements individuels (Zuboff, 2019). Une telle vision de l'organisation de la société numérique inspire une partie de la population à se détourner de ces espaces par manque de confiance, de peur d'être traquée par

(1) EDI : Échange de données informatisées ou *Electronic Data Interchange*, échange d'informations structurées par des messages automatiques entre deux entités, de machine à machine. Voir https://fr.wikipedia.org/wiki/Échange_de_données_informatisé

(2) Le taux de fraude pour les paiements en ligne avec une carte bancaire française s'élève à 0,167 % en 2019. Observatoire de la sécurité des paiements (2020), rapport annuel, 82 p., septembre.

(3) Baromètre du Numérique 2019, « Enquête sur la diffusion des technologies de l'information et de la communication dans la société française en 2019 », Credoc, CGE, Arcep, 250 p.

(4) Sondage Odoxa (2019), « Données personnelles. La "*privacy*" comme nouveau cheval de bataille de Google et Facebook », mai.

(5) Voir par exemple : RAHAL A. (2019), "Five data breaches to understand the importance of data security", *Cisomag,* https://cisomag.eccouncil.org/5-data-breaches-to-understand-the-importance-of-data-security/

les dispositifs technologiques de ces plateformes, comme les caméras de leur ordinateur, leur *smartphone* ou encore les enceintes connectées [6].

Cependant la surveillance de l'espace numérique ne se limite pas à l'analyse des comportements d'intention d'achat ou de consommation. Elle est également le fait des États et de leurs services de renseignement. Les révélations de Snowden ont permis de mesurer l'ampleur de cette surveillance étatique des communications électroniques [7]. Ces révélations ont jeté une suspicion généralisée sur l'espace numérique, affaiblissant d'autant la confiance que les utilisateurs pouvaient avoir en cet espace.

Dans ce monde « post-Snowden », l'espace numérique est également devenu un espace d'affrontements géopolitiques qui se caractérise par une escalade et une sophistication croissante des attaques qui visent aussi bien des acteurs économiques pour leur extorquer des fonds que des acteurs publics, comme des hôpitaux, mais aussi des systèmes électoraux. Ces attaques, dans un monde qui a basculé dans le tout-numérique à l'occasion de la pandémie, éprouvent les systèmes de sécurité et leur résilience. Elles questionnent la robustesse de ces systèmes et la confiance que l'on peut y placer.

Construire la confiance en ligne : des tiers de confiance à l'architecture du réseau comme infrastructure de confiance

Pour construire la confiance dans les services numériques, plusieurs dispositifs s'articulent, reprenant des mécanismes classiques de gestion de la confiance. La logique du tiers de confiance a ainsi été rapidement introduite, même si elle a évolué à mesure du développement du *web*, pour intégrer les logiques propres aux échanges virtuels. Plus encore, l'émergence du protocole *blockchain* pousse la logique réticulaire plus loin puisqu'elle définit le réseau lui-même comme tiers de confiance.

S'appuyer sur les logiques classiques de la confiance

Dans le monde des échanges physiques, la confiance s'appuie sur plusieurs dispositifs institutionnels comme les labels, les marques et la réputation. Ces dispositifs ont tous été repris dans l'espace numérique. Le commerce en ligne a dû développer de nombreux mécanismes, dont les labels, afin de rassurer les internautes qui ont été longtemps rétifs aux achats en ligne (Ratnasingham, 1998). De multiples labels ont ainsi été mis en place (Trusted e-shop, charte qualité Fevad, etc.) et ont été complétés par des labels spécifiques pour le paiement (VeriSign Trusted). À ce dispositif est venu s'ajouter la marque comme indicateur de confiance. Si celle-ci joue indéniablement comme un facteur de confiance pour déclencher une commande sur un site de vente en ligne, elle ne peut à elle seule suffire à garantir la confiance, la qualité de l'exécution et la logistique jouant un rôle crucial dans la confiance accordée à un site marchand, ce que certains acteurs ont su parfaitement anticiper pour en faire un puissant moteur de confiance. Cependant de tels mécanismes ne suffisent à eux seuls à garantir la confiance dans les transactions en ligne.

Adapter le tiers de confiance à l'ère numérique

Afin de garantir l'identité des parties et l'intégrité des transactions, et en l'absence d'une identité numérique substantielle, l'introduction d'un tiers de confiance est un mécanisme institutionnel classique qui a été répliqué dans l'espace numérique, sous forme de certificats électroniques

(6) CLAUSER G. (2019), "Amazon's Alexa never stops listening to you. Should you worry?", *New York Times*, 8 août, https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/
(7) SNOWDEN E. (2019), *Mémoires vives*, Le Seuil, 384 p.

délivrés par une instance aux parties dans une transaction. Si cette logique a pu être déployée dans les transactions B2B (*business to business*), elle a échoué à se développer dans les transactions B2C (*business to customer*) ou C2C (*customer to customer*), du fait de sa complexité technique pour les utilisateurs non professionnels.

Dès lors, plusieurs formes de tiers de confiance ont émergé pour fournir aux utilisateurs un cadre à leurs échanges. Un premier mécanisme est celui de l'évaluation par les pairs d'un produit, d'un service. Les évaluations de la foule et les avis clients, organisés, structurés et mis en valeur, constituent un puissant mécanisme de confiance. Les avis clients deviennent donc en tant que tels un dispositif de la confiance en ligne (Utz & alii, 2012). Cependant, ce mécanisme est lui-même susceptible d'être détourné par des acteurs malintentionnés. Le régulateur a donc introduit des contraintes spécifiques aux acteurs recourant aux avis clients [8]. Des modèles d'affaires se sont bâtis sur les avis clients comme Tripadvisor dans le voyage ou La Fourchette pour les restaurants.

De façon plus générale, les services de l'économie dite collaborative, pour lesquels il faut, par exemple, faire confiance à un chauffeur inconnu pour le covoiturage (Mazzela & alii, 2016), ou encore faire confiance à un inconnu locataire de sa maison (Hawlitschek, 2016). Dès lors, le rôle de la plateforme intermédiaire consiste à être le tiers de confiance, comme dans le modèle des places de marché. La plateforme fournit une infrastructure aux échanges. Elle sélectionne par des mécanismes de référencement les différents acteurs qui vont interagir, vérifie les identités, organise les avis clients et, de la sorte, construit un cadre de confiance plus ou moins élaboré, selon les plateformes (Isaac, 2021). Toutefois, un tel mécanisme centralisé, pour efficace qu'il soit, n'en connaît pas moins plusieurs limites. Il est toujours possible de biaiser les avis clients, d'en publier de faux. Aussi nombreux que puissent être les contrôles, la fraude sera toujours présente sur les plateformes.

Aussi, c'est par un dépassement de l'infrastructure de confiance centralisée, représentée par les plateformes, que d'autres alternatives de gestion de la confiance émergent.

La *blockchain*, ou le réseau comme mécanisme de confiance

Avec la technologie *blockchain*, le tiers de confiance devient le système lui-même (Werbach, 2016) : chaque élément réparti de la *blockchain* contient les éléments nécessaires à garantir l'intégrité des données échangées par un algorithme cryptographique. La chaîne de blocs est une base de données distribuée qui stocke et transmet des informations, envoyées par les utilisateurs. Les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne. Une chaîne de blocs gère donc une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage. À ce titre, c'est un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti. Ainsi, une telle architecture devient le tiers de confiance, réduisant d'autant les coûts de transaction liés à son existence. Contrairement aux contrats, les chaînes de blocs ne s'appuient pas sur un système juridique pour faire respecter les accords. Contrairement à l'utilisation de normes relationnelles, les chaînes de blocs ne nécessitent pas de confiance ou de relations directes entre les différents acteurs de la chaîne (Lumineau & alii, 2020).

Une telle architecture résout en partie les enjeux de confiance liés aux transactions numériques : elle offre aux transactions une infrastructure d'échange robuste. Elle apporte une traçabilité complète des échanges et une transparence pour les acteurs. Une telle architecture est donc souvent envisagée comme une solution aux nombreuses limites auxquelles la confiance se heurte dans l'espace numérique.

(8) https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/faux-avis-consommateurs-sur-internet

Si l'on perçoit bien l'intérêt pour les transactions marchandes, en revanche, une telle infrastructure ne renforcera en rien la confiance pour les autres contenus numériques, notamment les fausses informations. En effet, une telle infrastructure ne peut infirmer ou confirmer la véracité d'une information. Par ailleurs, elle ne supprime pas les questionnements autour de la surveillance des activités en ligne par les États.

L'espace numérique reste donc un espace où la construction de la confiance est un perpétuel défi, et où la technologie par elle-même semble rarement apporter les éléments suffisants pour bâtir un cadre de confiance robuste.

Références

COECKELBERGH M. (2010), "Humans, animals, and robots: A phenomenological approach to human-robot relations", *International Journal of Social Robotics*, 3(2), pp. 197-204.

HAWLITSCHEK F., TEUBNER T. & WEINHARDT C. (2016), "Trust in the sharing economy", *Die Unternehmung – Swiss Journal of Business Research and Practice*, 70(1), pp. 26-44.

ISAAC H. (2021), *Les business models de plateforme*, Vuibert, Paris, 272 p.

MAZZELLA F., SUNDARARAJAN A., D'ESPOUS V. & MÖHLMANN M. (2016), "How digital trust powers the sharing economy", *IESE Insight*, third quarter (30), pp. 24-30.

MÖHLMANN M. (2016), "Sharing economy: Building trust in P2P online marketplaces", *New York Computer Science and Economics Day*, New York.

LUMINEAU F., WANG W. & SCHILKE O. (2020), "Blockchain governance – A new way of organizing collaborations?", *Organization Science*, https://doi.org/10.1287/orsc.2020.1379

TADDEO M. (2009), "Defining trust and e-trust: Old theories and new problems", *International Journal of Technology and Human Interaction*, 5(2), pp. 23-35.

TADELIS S. (2016), "The economics of reputation and feedback systems in e-commerce marketplaces", http://faculty.haas.berkeley.edu/stadelis/Annual_Review_Tadelis.pdf

UTZ S., KERKHOF P. & VAN DEN BOS J. (2012), "Consumers rule: How consumer reviews influence perceived trustworthiness of online stores", *Electronic Commerce Research and Applications*, Vol. 11, pp. 49-58.

RATNASINGHAM P. (1998), "The importance of trust in electronic commerce", *Internet Research*, 8(4), pp. 313-321.

WERBACH K. D. (2016), "Trustless trust", SSRN: https://ssrn.com/abstract=2844409

ZUBOFF S. (2019), *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, PublicAffairs, 704 p.