La confiance à l'ère numérique commence par les mots

Par Côme BERBAIN
Directeur de l'innovation du groupe RATP

Le numérique est porteur d'une promesse de création de confiance entre personnes ou entités ne s'étant jamais rencontrées. Si elle semble donc en premier lieu d'ordre technique, la création, puis l'entretien, de la confiance nécessite un discours cohérent entre les finalités, les pratiques, les technologies et les organisations aussi bien sur le plan numérique que physique. Dès lors, ce discours devient lui-même un objet de confiance ou de défiance qui peut avoir des effets contraires aux intentions initiales. La construction et l'utilisation d'un tel discours impliquent l'ensemble des parties prenantes internes et externes des organisations, et demeurent des défis à relever pour créer la confiance à l'ère du numérique.

Une des premières promesses du numérique est la possibilité d'échanger de manière quasi instantanée avec n'importe quelle personne ou entité sur la planète, et de réaliser des transactions sans avoir jamais rencontré physiquement cette personne ou entité. Cette promesse est donc une promesse d'établissement quasi instantanée du niveau de confiance nécessaire à l'échange ou à la transaction sans rencontre préalable. Au-delà, le numérique est progressivement devenu un élément courant dans la vie quotidienne qu'il s'agisse du travail, du commerce, de l'industrie, des démarches administratives, de l'information, de la culture... Il génère en lui-même des problématiques de confiance : gestion des données personnelles, confiance dans les algorithmes mis en œuvre, cybersécurité, possibilité d'ingérence étrangère légale dans les systèmes, diffusion massive de fausses nouvelles, et manipulations.

La question de la confiance à l'ère numérique est donc autant celle du numérique lui-même que de l'insertion du numérique dans des systèmes mêlant physique et numérique. La génération de cette confiance, si elle s'appuie sur des dispositifs techniques ou organisationnels ne peut avoir lieu sans discours. C'est dans un discours cohérent et orienté vers les utilisateurs et les communautés que se trouve un élément indispensable de la confiance. Ce discours finit par devenir un élément propre de confiance ou de défiance de ses destinataires, capable de renforcer ou d'amoindrir en retour la confiance en un produit, un service ou une institution. La conception, la production et la maitrise dans le temps d'un discours générateur de confiance est un élément clé, qui dépasse la seule activité habituelle de communication.

La confiance suppose un discours aligné avec les finalités, les pratiques, les technologies et les organisations

Le développement rapide du numérique dans les différents pans de l'activité économique et administrative a permis la mise en place de transactions rapides, simples et fluides, en évolution constante. Pour cela, un ensemble de politiques, de processus, de technologies et

d'organisations sont mises en place qui peuvent se répartir en quatre niveaux : le système d'information (SI) ; les données collectées et utilisées ; les algorithmes mis en œuvre ; et les informations fournies à l'utilisateur et les interactions associées.

L'utilisateur final n'a pas la capacité de mesurer finement les aspects numériques de ces transactions, et doit donc s'en remettre à un discours pour accorder ou non sa confiance à un service en ligne pour plusieurs raisons.

En premier lieu, l'utilisateur n'a le plus souvent pas accès aux éléments nécessaires (code, structure de données, architecture du SI, documents de politique...). Plusieurs approches visent à compenser ce manque d'accès aux informations. Le mouvement *open source* publie les codes des logiciels, et donc vise à les rendre accessibles et auditables. Néanmoins, l'utilisation de ce code dans un service donné implique des choix de versions et d'intégration qui peuvent considérablement modifier l'utilisation du logiciel et amoindrir, voire annuler le bénéfice de l'ouverture de code.

Par ailleurs, la règlementation a introduit des obligations d'informations et de fourniture d'éléments en matière de données personnelles *via* le RGPD, ou de transparence des algorithmes en ce qui concerne une partie conséquente de la sphère administrative. Elle crée donc une obligation de porter un discours spécifique vers les utilisateurs de ces services. Cependant, indépendamment de la réalité de leur mise en application réelle, ces éléments, s'ils sont déterminants en matière de confiance, ne sont toutefois pas suffisants.

En second lieu, quand bien même il y aurait accès, l'utilisateur n'a généralement pas les compétences nécessaires ni le temps pour évaluer l'ensemble des éléments. Le numérique a créé des tiers de confiance pour répondre à cette problématique, notamment au travers de processus d'audit, ou de certification. Outre que ces processus nécessitent des temps longs et impliquent des montants élevés, ils sont également intrinsèquement limités par rapport à l'évolution rapide des services, et contribuent en pratique à développer un discours visant à générer de la confiance.

Enfin, une partie des éléments à évaluer ne peuvent l'être qu'en situation de crise ou dépendent de capacités futures : lorsqu'un utilisateur permet à un commerce en ligne d'enregistrer un numéro de carte bleue, il place sa confiance dans la capacité du commerce à protéger cette information dans le présent, mais aussi dans le futur, à détecter les attaques cyber le cas échéant, à l'informer d'une possible fuite de donnée. Par ailleurs, il fait également confiance à sa banque pour bloquer rapidement toute transaction frauduleuse. Une telle évaluation pourrait se faire sur les compétences des équipes en place ou les processus et politiques associées, mais resterait fortement dépendante des évolutions de l'entreprise concernée. Elle est donc tributaire des déclarations existantes de l'organisation concernée.

Compte tenu de son incapacité à évaluer formellement un service, l'utilisateur va donc se raccrocher à ce qu'il peut capter, pour choisir de placer sa confiance en tel ou tel service : qualité de l'interface utilisateur, fonctionnement du service et présence de *bug*, échanges avec le service client, évaluation du service par d'autres utilisateurs, certification partielle par des tiers, cohérence des éléments avec la finalité du service, notoriété globale…

Un discours générateur de confiance est par conséquent une construction impliquant l'ensemble des éléments constituant le service, et visant à aider l'utilisateur à placer sa confiance dans le service en question. Bien loin d'être un seul élément de marketing ou de communication, il concerne et nécessite l'implication de l'ensemble des équipes de l'organisation qui produit le service.

Ce discours doit en premier lieu être adapté au service : le besoin de confiance n'est pas le même pour une démarche administrative et pour l'achat d'un NFT (*non-fungible token* ou jeton non fongible) en ligne. La confiance de l'utilisateur peut donc être limitée sans que cela ne soit gênant pour l'utilisation du service : certains utilisateurs accepteront de

réaliser un acte d'achat auprès d'un *e*-commerçant sans pour autant accepter l'enregistrement de leur numéro de carte de crédit. Ils font confiance à la plateforme pour délivrer une fois un produit sans pour autant accorder une confiance de long terme.

Le discours doit être cohérent avec les moyens techniques et organisationnels : rien n'est pire que de recevoir des injonctions contradictoires ou de constater que les informations affichées par le service numérique sont fausses. Cela reste vrai, que le service passe par une entreprise avec un service client ou par une communauté organisée autour d'une *blockchain* : une réponse inadaptée du service client ou la modification unilatérale d'un des algorithmes de la *blockchain* entraine la même perte de cohérence du discours, et donc la diminution de la confiance accordée.

À défaut de cohérence, certaines pratiques d'un service vont limiter la confiance des utilisateurs : il est connu que Meta pratique une utilisation extensive des données de ses utilisateurs. Cela n'empêche cependant pas un grand nombre d'utilisateurs de faire confiance à Meta pour des fonctions précises (réseau social, informations…), en acceptant ou en tentant de limiter les autres utilisations que Meta peut faire de leurs données. Le discours qu'essaye de promouvoir Meta sur le respect des données personnelles et la sécurité de sa plateforme se heurte à l'expérience des utilisateurs et les fuites dans la presse d'éléments contradictoires ("Cambridge Analytica", témoignage de Frances Haugen…). En conséquence, ce discours n'est pas pris au sérieux par les utilisateurs qui limitent la confiance qu'ils placent en Meta.

Le discours de confiance devient lui-même un enjeu de confiance ou de défiance

Au-delà de sa cohérence avec le service numérique, le discours de confiance peut faire l'objet d'une mise en scène visant à le démontrer au-delà du service lui-même. C'est le cas de nombre de services qui vantent leur protection des données personnelles de leurs utilisateurs et le chiffrement de bout en bout. Si une véritable démonstration, même partielle de cette protection, est difficile à établir, il est extrêmement rare de voir publier des éléments probants, que ce soit sous forme d'audit ou de certification de sécurité. En la matière, le discours essaye de se passer de preuves liées au service lui-même.

Dès lors, pour tenter d'étayer ce discours, il est possible de recourir à des éléments externes, ainsi que l'a fait Apple en contestant en justice des demandes du FBI sur des accès à des données. Au-delà du cas lui-même, Apple utilise cette contestation pour appuyer son discours sur la protection des données, en indiquant à ses clients et futurs clients que l'entreprise est prête à défier le gouvernement américain pour protéger leurs données.

De même, les politiques de gestion des *cookies* au sein des navigateurs Internet ont fait l'objet d'une surenchère après les obligations d'affichage mis en place par la Commission européenne en 2018. Les principaux développeurs de navigateur souhaitant attirer le plus d'utilisateurs possibles, et ayant pour cela besoin de leur confiance, ont fait des déclarations importantes pour limiter le rôle des *cookies* ou pour fournir des moyens aux utilisateurs de les maîtriser. Ces déclarations n'ont pas toujours été suivies d'effet ou alors d'effet limité : l'intégration d'un outil complexe à utiliser dans certains navigateurs permet effectivement d'améliorer la situation comme promis, mais suppose un temps conséquent de paramétrisation de la part des utilisateurs. Dans ce cas, le discours vise surtout à générer de la confiance en matière de vie privée plutôt qu'une réelle efficacité d'amélioration de cette vie privée.

De plus, les innovations numériques dans le domaine de la *blockchain* se présentent comme des éléments générateurs naturels de confiance. "*Smartcontract*", NFT, "*web3*" : tous ces termes se présentent comme reposant sur des mécanismes inviolables et surfent sur des effets de mode pour survendre une confiance qui est peu ou pas établie. Il est à

prévoir un renversement sur un certain nombre de ces sujets, comme il vient d'avoir lieu sur les NFT. Une survente de la confiance finit par avoir un effet inverse.

Le discours peut également directement diminuer la confiance des utilisateurs en matière numérique. La médiatisation de comportements négatifs (arnaques en lignes, détournements de numéro de cartes bleues), si elle permet la sensibilisation, est souvent présentée de manière exagérée et peut créer des effets négatifs en matière de confiance.

De plus, l'effet Streisand est maintenant bien documenté : la communication sur un élément que l'on souhaite retirer peut lui donner une popularité largement supérieure allant ainsi à l'encontre de l'objectif initial de la communication. Si cet effet n'a pas attendu le numérique pour apparaitre, les outils numériques, et notamment les réseaux sociaux, permettent sa démultiplication à la fois en termes de fréquence d'apparition et d'ampleur.

Dans certains cas, ce sont les termes même employés dans le discours qui peuvent diminuer la confiance : c'est le cas de la « reconnaissance faciale », qui, compte tenu de sa connotation négative et de son utilisation par des régimes autoritaires, entraine une défiance. Le terme de « reconnaissance faciale » est largement utilisé dès lors qu'une reconnaissance de forme est couplée à une caméra, et ce alors même que nombre des traitements limités ne font pas techniquement appel à la reconnaissance d'un visage, ni même d'un individu. C'est le cas par exemple de la détection d'obstacle devant un véhicule ou de l'évaluation de la densité de personnes sur un quai, pour lesquels il n'est pas besoin de reconnaitre les individus de manière unitaire. En conséquence, des limitations importantes de ces dispositifs sur le plan de l'acceptabilité sociale ou de la règlementation sont mises en place allant même jusqu'à obtenir l'effet inverse de celui recherché par la loi : pour permettre l'exercice du droit d'opposition des citoyens sur de tels systèmes, il peut devenir nécessaire dans certains cas de développer une reconnaissance faciale des individus exerçant ce droit pour pouvoir les exclure du traitement. Une analyse fine des différents types de traitement et un discours permettant de prendre en compte la complexité associée sont à même d'éviter de telles aberrations.

Au-delà d'un effet positif ou négatif du discours sur la confiance, il est à noter un cas particulier : celui du non-discours comme facteur de confiance : pour éviter un effet Streisand, il peut être plus intéressant de ne pas communiquer. De même, en matière de cybersécurité, la publication de la détection d'une attaque peut agir comme un facteur de confiance ou de défiance, en fonction de l'organisation concernée et de l'étendue de l'attaque. Il est alors fréquent que celle-ci ne communique pas de manière publique ou déploie un discours vide de contenu renvoyant aux autorités pour permettre de gérer au mieux l'attaque.

Enfin, certains champs du discours restent à construire en parallèle des dispositifs techniques. C'est le cas en matière d'intelligence artificielle : si les technologies d'IA certifiées commencent à émerger et à sortir des laboratoires de recherche, les débats actuels sur les jeux de données et leur caractère représentatif de la population montrent bien que l'IA de confiance n'est pas encore un élément correctement défini et pour lequel le discours n'est pas totalement construit. Il s'agit encore d'un sujet de recherche et de développement.

Conclusion

Si elle semble en premier lieu d'ordre technique, la confiance dans le numérique passe par un discours aligné sur les finalités, les pratiques, les technologies et les organisations mises en place. Le discours de confiance est fragile et peut facilement avoir des effets pervers d'autant plus qu'il doit être cohérent dans le temps, et ce alors même qu'une partie des technologies et de leurs utilisations sont en cours de création et d'évolution. La construction et l'utilisation d'un tel discours impliquent l'ensemble des parties prenantes internes et externes des organisations (qu'elles soient entreprises, administrations, communautés…), et demeurent des défis à relever pour créer la confiance à l'ère du numérique.