Introduction

Par **Côme Berbain**
Directeur de l'Innovation du groupe RATP et directeur du programme « Véhicule autonome »
et **Bertrand Pailhès**
Directeur des Technologies et de l'Innovation de la CNIL

« Faire confiance ». Alors que les rapports sociaux semblent se tendre et les repères hérités de la société industrielle disparaître, alors que le numérique constitue un des principaux facteurs de cette transformation des sociétés modernes, « faire confiance » est un *mantra* que peu de responsables politiques ou d'experts pourraient prétendre revendiquer. Et pourtant, le déploiement de la société de l'information depuis 30 ans a permis la constitution d'avancées aussi majeures pour le progrès que l'encyclopédie Wikipédia, bâtie par des milliers d'anonymes sans lien personnel entre eux, de nouvelles technologies fondées sur un *consensus* scientifique global ou le développement d'outils informatiques ouverts, au service de tous.

La confiance dans le monde numérique est une notion mal définie, dans laquelle des intérêts divers se retrouvent, selon que l'on parle de technologies, de contenus ou de contributeurs. Dans de nombreux cas, c'est avant tout une question de règles, de procédures et de standards acceptables par tous et dont le respect conditionne un engagement sincère et sécurisé par chacun. Ces règles sont parfois facilitées par les technologies comme le chiffrement asymétrique, et reposent, dans d'autres cas, sur la pratique des organisations et des individus. Ainsi, à la fin du XX^{e} siècle, alors que la « netiquette » prétendait transposer les standards de la cordialité sociale au monde numérique, ces dernières années ont plutôt mis en lumière les abus, la haine en ligne et le complotisme dans un mouvement de relativisation générale de la vérité par la magie de l'accès instantané, démontrant ainsi la fragilité des mécanismes de confiance dans le numérique.

C'est bien toute l'ambivalence des effets du numérique qui s'exprime à nouveau à travers ce sujet polysémique. Il semble aujourd'hui pertinent de revenir sur les dynamiques qui contribuent ou, au contraire, nuisent à l'émergence d'un numérique de confiance. Avant de plonger dans les dernières technologies ou les régulations qui cherchent à répondre aux défis actuels, il est utile de revenir sur les ressorts de la confiance en s'intéressant au regard que porte la psychologie sur ce sujet ou bien à l'importance de la procédure dans le système judiciaire. Ces points de vue illustrent notamment deux dimensions cardinales de toute relation de confiance : la stabilité et la transparence. En effet, la confiance dans le numérique repose, d'abord, sur une construction patiente, qui se renforce avec le temps et qu'aucune action sur le court terme, aussi décidée et légitime qu'elle soit, ne peut concurrencer. Elle dépend, ensuite, de la visibilité donnée sur le processus, l'algorithme ou l'entité qui prétend la gagner : que ce soit pour les SI (systèmes d'information) de l'État, les réseaux sociaux ou un algorithme de chiffrement, l'opacité n'a jamais pu constituer une approche durable.

Ce numéro de *Enjeux numériques* souhaite ainsi explorer les différentes approches proposées aujourd'hui pour renouer le lien de confiance entre usagers, entreprises et institutions en commençant par les approches technologiques, mises en regard des évolutions réglementaires et du rôle des institutions.

En effet, les avancées du numérique reposant majoritairement sur les possibilités apportées par la technologie, il est particulièrement séduisant d'essayer d'apporter une réponse technique à la question de la confiance. Cette réponse peut se fonder aussi bien sur l'évaluation technique au

travers de méthodes sophistiquées de certification que sur la tentative de l'intégration partielle ou totale de la dimension « confiance » dans la technologie : le développement des technologies de cryptographie homomorphe ou de l'IA de confiance montre que ces pistes sont prometteuses, mais pas encore suffisamment matures pour pouvoir générer de la confiance par leur seule utilisation. Les technologies *blockchain* constituent une autre tentative de générer de la confiance à partir de la seule technologie, en visant à remplacer le tiers de confiance par un protocole technique.

Cependant, comme illustré par l'adage commun en matière de cyberespace « la faille principale se trouve entre le clavier et l'écran », il est probablement illusoire de vouloir faire reposer la confiance à l'ère numérique sur la seule technologie. Élément indispensable, elle ne peut à elle seule capturer l'ensemble des facteurs humains, comme le montrent le succès régulier des attaques par *phishing* ou les détournements de Bitcoins qui ont lieu sans atteinte à la technologie employée mais en jouant sur des ressorts non numériques bien connus de crédulité ou d'appât du gain. Par ailleurs, la technologie qui tente d'intégrer la confiance possède également l'inconvénient d'être plus lourde, plus lente et plus complexe à mettre en œuvre. Dans un monde numérique dans lequel la simplicité pour l'utilisateur et la vitesse d'exécution priment sur les garanties, ces technologies sont *de facto* désavantagées. Qui lit les petites lignes de l'analyse de sécurité d'un produit cyber ? Ou s'intéresse aux détails d'implantation d'un protocole de chiffrement d'une messagerie qui vante de la sécurité de bout en bout ? Ce sont pourtant ces détails qui peuvent créer ou, au contraire, détruire la confiance, qui devient dès lors supposée par l'utilisateur et donc davantage une affaire de *marketing* et d'image qu'une réalité technique.

Les limites d'une approche purement technologique appellent par conséquent à des modes d'action complémentaires pour encadrer le développement de systèmes et de solutions informatiques rapidement perçus comme « complexes ». Dès les années 1970 et le grand débat national sur l'informatisation de la société, il a semblé pertinent de prévoir des garanties juridiques à l'utilisation de l'informatique. La loi Informatique et Libertés de 1978, mais également la loi CADA (qui a créé la Commission d'accès aux documents administratifs) la même année et la loi Archives l'année suivante, ont conclu ce travail de réflexion en posant des principes à respecter, dont les énoncés sont à la portée de tous : finalité du traitement des données, proportionnalité, sécurité, durée de conservation, transparence des décisions automatiques, notamment dans le secteur public. Ainsi, l'ensemble des idées qui restent pertinentes aujourd'hui avaient déjà été identifiées il y a plus de 40 ans.

Évidemment, l'arrivée d'Internet et l'utilisation du numérique dans tous les domaines de l'activité humaine ont accentué l'importance de ces mécanismes de confiance et ont conduit à un renouvellement des pratiques et des moyens : le RGPD (le règlement général sur la protection des données) a consacré le droit à la protection des données en renforçant les moyens de protection ; le mouvement de l'ouverture des données (*open data*) a étendu le principe de l'accès à toutes les données d'intérêt public et mené à de nouvelles approches fondées sur des communautés actives et organisées, avec l'ambition d'appliquer les principes de gouvernance des « communs » aux ressources numériques essentielles pour tous. Ces réflexions s'étendent aujourd'hui à la régulation des algorithmes, combinant preuves mathématiques, garanties procédurales et approches interdisciplinaires pour en capturer la complexité.

Plus récemment et à la faveur de la domination d'une « deuxième génération » de services en ligne fondés à la fois sur d'innombrables contributeurs et le rôle-clé d'un nombre limité de plateformes, la question de la confiance dans les informations diffusées en ligne se pose de manière aiguë. Si l'exemple de Wikipédia a montré la possibilité d'une gouvernance raisonnée de l'information (non exempte de critiques), le cocktail d'autorités publiques en mal de crédibilité, d'acteurs économiques mus par des intérêts économiques fondés sur la vente de publicité et de groupes d'intérêt organisés pour servir certains faits ou théories, est particulièrement dangereux et soulève

de nouvelles questions, techniques, institutionnelles et juridiques. Les développements récents en Europe et aux États-Unis apporteront peut-être des éléments de réponse sur les nouveaux équilibres à trouver sur ce sujet délicat.

Ce questionnement sur la gouvernance de l'information met en particulier en avant la question du rôle des acteurs publics dans la génération de la confiance numérique et celle de la forme de confiance numérique à laquelle ces acteurs peuvent prétendre. La transposition dans l'espace numérique d'un des principaux éléments de la confiance, l'identité des personnes physiques, est également une des problématiques sur lesquelles, dans le même temps, les acteurs publics ont une grande possibilité d'action et rencontrent en France des résistances élevées. Bien que nombre d'autres pays aient réussi le déploiement de solutions d'identité numérique, rares sont ceux pour lesquels cette identité a été déployée largement au-delà de la sphère publique. On assiste aujourd'hui à la gestion de l'identité en ligne autant, si ce n'est plus, par certains acteurs du numérique (Google ou Facebook) que par les États, soupçonnés par ce moyen de vouloir utiliser les possibilités du numérique pour exercer un contrôle étroit de la population. On retrouve cette dualité dans le cas de l'application StopCovid, entre un État qui cherche une souveraineté dans une application maîtrisée, mais qui a des difficultés à déployer un système technique et un accompagnement politique générateur de confiance tandis que Google et Apple déploient très rapidement un système techniquement très performant, mais dont le contrôle démocratique est totalement absent. Il est d'ailleurs intéressant de constater que les autres États européens ne portent pas le même regard que nous sur ces sujets.

S'ils ne peuvent ni créer techniquement les conditions de la confiance, ni réussir à la générer pour leurs propres applications, les pouvoirs publics ont cependant des champs d'action à investir. En rendant accessible le numérique à tous, par une politique ambitieuse d'inclusion numérique, en développant la régulation des espaces de dialogue en ligne, pour tenir un rôle de garant des équilibres entre la liberté d'expression et ses limites, rôle qui est aujourd'hui contesté par les grandes plateformes, les acteurs publics peuvent trouver une place et faire valoir la légitimité et la confiance que procure la démocratie.