

LE NUMÉRIQUE DE CONFIANCE EST UN SUJET POLITIQUE

Bénédicte PILLIET

► Présidente du Cybercercle



Le numérique imprègne aujourd'hui l'ensemble de la société. Il est au cœur des transformations de nos économies, influant sur les modèles anciens, créant de nouveaux métiers et filières, et en détruisant d'autres. Il influe sur nos usages professionnels, nécessitant l'acquisition continue de nouvelles compétences.

Il bouleverse nos usages personnels, avec une place de plus en plus grande donnée aux outils numériques, modifiant nos manières de nous informer avec le développement des réseaux sociaux qui tendent à se substituer aux modes traditionnels d'information ; de consommer, avec le développement des achats en ligne ; de nous soigner avec le recours accru à la téléconsultation, aux plateformes de réservation de rendez-vous médicaux et l'accroissement de la

e-santé jusqu'à la télé-chirurgie. Il modifie même nos modes relationnels avec le développement des échanges en visio ou via des messageries instantanées, qui assurent chez les jeunes générations des liens permanents avec leur « communauté ». Le numérique entraîne également une certaine inversion de la transmission de la connaissance entre générations, les plus jeunes aidant très souvent les aînés à apprivoiser ces nouveaux outils.

Le numérique est également un facteur clé de la transformation de nos institutions. Il est au cœur de l'évolution de l'organisation de l'Etat, tant interne qu'à destination des citoyens, avec des processus accélérés de dématérialisation pour la plupart des actes administratifs. Il modifie également la manière dont les collectivités envisagent les services publics et les rapports avec leurs administrés avec le développement du concept de e-citoyen. Il modèlè l'espace public, notamment à travers les territoires connectés, permettant via le recours à de multiples capteurs et à l'intelligence artificielle, d'optimiser les ressources, d'améliorer la sécurité et d'adapter les services dans un objectif de transformation écologique, que ce soit en matière de gestion de l'éclairage, des transports, de l'énergie...

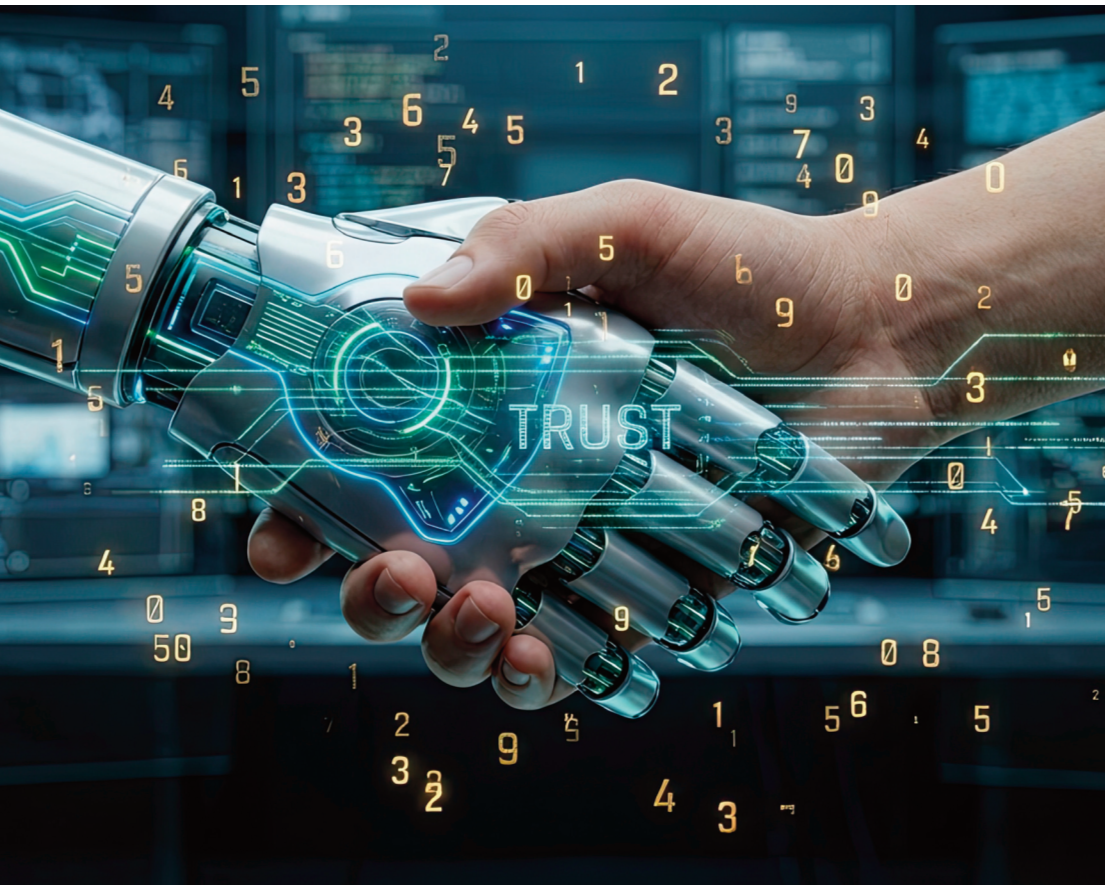
« Le numérique imprègne aujourd'hui l'ensemble de la société. »

Il est enfin devenu pour les états un enjeu de puissance au cœur de laquelle indépendance et souveraineté ont été rendus plus prégnants par le durcissement des relations internationales.

Une transformation profonde à tous niveaux, que l'accélération des technologies avec la « révolution » de l'intelligence artificielle et celle à venir du quantique, comme le rôle accru de la donnée dans la création de valeur et un renforcement de la compétition internationale, viennent encore complexifier.

Cette transformation numérique de nos sociétés a entraîné de fait une augmentation des risques auxquelles citoyens, entreprises, administrations de l'Etat et collectivités, associations et autres organisations sont confrontés. Il n'est pas une seule semaine sans que paraisse un article relatant une cyberattaque ayant ou non entraîné des fuites de données, ou que nous soyons confrontés à titre individuel à un courriel ou un sms frauduleux. Car ce développement du numérique a aussi créé un nouveau « marché » pour les cybercriminels qui sont de plus en plus organisés, créatifs, et « professionnalisés ».

Dans ce contexte une évidence s'impose : pour que la transformation numérique qui est la nôtre produise tous ses bénéfices, la sécurité et la confiance numériques se doivent d'être assurées. Il n'y a pas aujourd'hui de développement ou



de croissance sans numérique, de numérique pérenne sans confiance et de confiance sans sécurité numérique.

Or nous faisons face aujourd'hui à un paradoxe : le numérique n'est pas aujourd'hui considéré par les élus comme un sujet politique. Et moins encore le numérique de confiance. Souvent considéré comme un sujet relevant uniquement des « experts », il est absent des programmes électoraux et n'est présent dans les discours des élus que pour traiter de la nécessité d'une souveraineté-autonomie européenne traitée théoriquement ou pour glorifier la réussite de licornes - qui trop souvent d'ailleurs désertent outre-Atlantique. Le numérique n'est pas vu comme ce qu'il est devenu : le facteur clé de la transformation de la société, de l'économie, des rapports sociaux, posant de fait un sujet fondamental : quel type de société souhaitons-nous ?

Ainsi on cherchera vainement dans les discours politiques des dix dernières années une vraie stratégie en matière de numérique, pour sa sécurité ou la confiance que tout citoyen pourrait attendre de son utilisation. Et si l'on doutait encore de la prise en compte au bon niveau politique du numérique, il suffirait de regarder le rang protocolaire des secrétaires d'État ou des ministres en charge du numérique des gouvernements de ces dernières années : non rattachés directement au Premier ministre, ce que le sujet éminemment transverse du numérique légitimerait et, sauf exception, sans autorité sur les administrations nécessaires à l'action.

Autre paradoxe : alors même que le politique se saisit peu de cet enjeu, organismes de contrôle ou réglementation ne cessent de proliférer, en particulier en matière de sécurité numérique, sous l'influence depuis une dizaine d'années de la dynamique inflationniste de l'Europe. NIS1, NIS2, CRA, DSA, DMA, CSA, DORA, REC... autant d'acronymes qui recouvrent des législations qui certes visent l'objectif vertueux de renforcer le niveau global de sécurité numérique, mais dont les effets de bord peuvent être contre-productifs au niveau économique, social voire démocratique.

Ainsi en est-il également de la création en France de Viginum pour lutter contre les ingérences étrangères et du DSA (Digital Service Act) européen créé pour combattre la désinformation. En France des utilisateurs de réseaux sociaux sont désormais poursuivis en justice pour ce qu'ils ont écrit ou dit, bien au-delà des propos condamnés habituellement par

la loi - lois de 1881, Gayssot, traitant les atteintes à la vie privée, à l'image, à la présomption d'innocence, au secret professionnel, l'apologie de crimes ou du terrorisme, etc.

On le voit, le numérique de confiance est aujourd'hui, avec les thématiques intrinsèques qui sont les siennes, au cœur de ce qui relève du Politique.

Au vu des enjeux, il est temps pour les élus de se saisir pleinement de ces sujets. 2027 représente ainsi une opportunité de traiter le numérique de confiance au niveau auquel il doit l'être : au plus haut. ●

« Il n'y a pas aujourd'hui de développement ou de croissance sans numérique, de numérique pérenne sans confiance et de confiance sans sécurité numérique. »

La souveraineté numérique ne se décrète pas. Elle s'incarne.

Face aux menaces cyber, la technologie n'est qu'un outil. Le véritable acteur de défense de nos institutions, c'est l'humain. Hucency place les agents au cœur de la stratégie de défense nationale. À travers des programmes d'entraînement de haute précision, nous bâtissons une culture de la vigilance pour protéger durablement le service public et l'intérêt général.

**Donnez un sens à la cybersécurité.
Scannez et découvrez l'ADN de Hucency.**



Membre partenaire du

