Données personnelles : mettre fin à la politique de l'autruche

Laurane RAIMONDO

DPO
Chercheure associée au CLESID

A la mi-novembre 2020, Pôle Emploi ne proposait que trois postes de délégué à la protection des données à l'échelle nationale. Un chiffre qui en dit long sur la manière dont le sujet est perçu au sein des organismes. Largement considérée comme un « empêcheur de tourner en rond », la législation en la matière peine encore bien trop à être appliquée tandis que nous sommes à un carrefour essentiel entre nécessité d'utiliser les données et nécessité de les protéger.

Au-delà des lois, la protection de données à caractère personnel repose sur deux piliers principaux : la cybersécurité et le comportement humain.

Mettons-les en œuvre : déconstruisons l'idée que la protection des données comme la cybersécurité sont affaires des seuls techniciens, édifions une conscience commune, enseignons et accompagnons la population dès les premiers contacts avec les outils numériques. Nous en serons payés de retour.

Faire en sorte que tous se sentent concernés est peut-être ce qu'il y a de plus difficile à mettre en œuvre. Il s'agit ni plus ni moins du levier qui nous fera basculer vers un univers numérique plus sûr en renforçant les remparts bâtis autour du droit fondamental relatif à la vie privée. Prédomine pourtant le traditionnel « je n'ai rien à cacher » concernant ses propres données et un faux sentiment de sécurité se répercutant dans le cadre professionnel. Dissocier l'aspect privé et professionnel de la protection des données est une erreur : qui ne se soucie pas de ses données sera peu attentif à celles des autres et la seule peur de la sanction en cas de violation au sein de son entreprise ou administration a démontré son inefficacité. Il est également certain qu'une personne n'ayant pas de notion d'« hygiène numérique » présente à l'attaquant deux surfaces d'exposition lorsqu'elle ne crée pas de mur de sécurité entre sa vie privée et sa vie professionnelle, utilisant des mots de passe identiques ou se servant de ses outils professionnels pour gérer des aspects de sa vie personnelle et vice versa.

De cette perception tronquée insinuant l'idée que la protection des données ne concerne que quelques-uns, celle d'une cybersécurité cloisonnée aux seuls techniciens est tout aussi problématique. Là encore, elle est affaire de tous. Une forteresse n'est pas imaginée, dessinée, financée, construite, entretenue et défendue pas

une seule personne ni même une équipe restreinte, mais par un ensemble d'acteurs connaissant chacun leur rôle, de l'architecte qui en fait une place forte solide aux gardes qui en filtrent les entrées en passant par ceux qui en assurent l'entretien. Il suffit d'une faille pour faire tomber la plus robuste des forteresses comme tout système bien construit. La seule inattention ou faiblesse d'un mot de passe suffiront à laisser le chaos s'insinuer dans le système d'information le plus sécurisé qui soit. Comment douter encore aujourd'hui de la nécessité d'impliquer tous les acteurs d'un organisme ?

Une cyberattaque donnant lieu ou non à une violation de données n'a pas que des conséquences en termes de continuité d'activité, de réputation ou de chiffre d'affaire, c'est comme se retrouver face à son domicile cambriolé : solitude ; détresse et impuissance de la victime. L'écran devient noir et ce n'est qu'à ce moment qu'elle se rend compte de la fragilité du système autant que de sa dépendance à celui-ci. Plus que des outils, le smartphone, l'ordinateur ou la tablette sont devenus des prolongements de nous-mêmes et de nos activités à un point suffisamment élevé pour que leur sécurité soit prise au sérieux à degré équivalent : une véritable conscience collective doit se développer autour de la sécurité des données personnelles et des outils numériques.

Le premier smartphone atterrit entre les mains d'un enfant en moyenne entre 10 et 12 ans, s'ensuit une découverte des ressources du cyberespace avec un contrôle extrêmement limité de la part d'adultes souvent eux-mêmes dépassés par les possibilités de ces outils. Les habitudes d'usages s'adoptent tôt, les mauvaises plutôt que les bonnes auront tendance à perdurer si n'est pas rapidement développé un enseignement commun et régulier dès l'entrée au collège. Faire des prochaines générations des citoyens responsables face à des outils pouvant se révéler dangereux pour eux autant que pour les autres est plus qu'une nécessité, c'est un devoir. Il en va de même avec des adultes ayant vécu l'implémentation progressive du numérique dans leurs organismes comme dans leur vie privée.

Il est courant de constater que ces personnes ont automatisé et rationnalisé les gestes quotidiens nécessaires à leur activité professionnelle : lire et répondre aux e-mails ; utiliser Word ; envoyer des documents, éventuellement utiliser un logiciel de travail et c'est tout. Elles fonctionnent avec un enclos de sécurité, ne sortent pas du minimum indispensable, sont ancrées sur leurs appuis et de fait, ne développent aucun réflexe de sécurité. La peur de cliquer sur quelque chose qui modifierait le fil du fonctionnement sécuritaire inhibe la curiosité naturelle de l'être humain.

Les forces et faiblesses des outils numériques se situent au même endroit : l'invisibilité du mécanisme. Il y a quelque chose de « magique » à écrire des mots sur un clavier qui parviendront en quelques secondes à un destinataire localisé de l'autre côté de la planète, mais combien sommes-nous à savoir précisément comment tout cela fonctionne ? La réponse à la plupart de nos problématiques se trouve dans cette question. L'absence de connaissances, la division des tâches et l'imperméabilité des informations sont davantage responsables que la direction d'une entreprise traînant à prendre des mesures concrètes en matière de sécurité des données et du système ; qu'un employé manquant de bon sens ou qu'un Etat ne prenant pas suffisamment en main la sécurité numérique globale des organismes relevant de sa juridiction.

De la connaissance jaillira la conscience collective, il s'agit à présent de partager le plus largement

possible le seul bien que l'on ne perd pas en le diffusant : le savoir. Toucher toutes les strates de la population utilisant des outils numériques c'est puiser dans toutes les ressources qu'il est possible de mettre en place : l'enseignement pour les plus jeunes ; la formation pour les adultes et les professionnels ; les avantages fiscaux pour les entreprises et jeunes entrepreneurs du secteur ; l'investissement de la sphère sociale pour les personnes en difficulté, chose qui est d'ailleurs en route avec l'annonce du recrutement de 4 000 conseillers numériques par l'Etat. Nous aurons respectivement à la clef : des jeunes qui sauront protéger leurs propres données et celles qu'ils seront amenés à manipuler plus tard ; des actifs vigilants et pleinement acteurs de la sécurité des données et du système de l'organisme pour lequel ils travaillent ; une offre assez importante pour répondre à des demandes plus nombreuses et précises ; une nouvelle économie stimulée par l'émergence de nouvelles activités qu'il nous appartient de créer et enfin, des personnes vulnérables pouvant bénéficier d'un accompagnement de qualité.

Le moment est idéal pour se convaincre de l'utilité de tout investissement visant à sensibiliser, former et accompagner l'ensemble la Nation aux enjeux autour de la sécurité numérique et de la protection des données. L'optimisme doit prévaloir en la matière, il n'est pas trop tard pour affirmer haut et fort que ces problématiques nous concernent tous autant que nous sommes et qu'il est temps de sonner le tocsin. L'émergence d'une conscience collective permettra à la France de construire une véritable forteresse numérique aux frontières elles aussi invisibles et dessinées par sa propre population.

Alors qu'attendons-nous ?