Le RGPD au service de la cybersécurité

Par **Jean LESSI**
Commission nationale de l'Informatique et des Libertés (CNIL)

La cybersécurité, première des libertés informatiques ? Il n'est sans doute pas opportun de souhaiter à cette formule, dans le monde numérique, le succès que celle dont elle s'inspire a connu dans le monde physique. Les premières des libertés, à l'ère informationnelle, ce sont, plus que jamais, le droit au respect de la vie privée et le droit de chacun à maîtriser les usages faits de ses données personnelles. Mais l'on sait que, sans mesures appropriées de sécurité, et, plus encore, sans une culture profondément partagée de la cybersécurité, ces libertés individuelles sont des plus fragiles.

Cybersécurité et protection des individus, même combat

Ce n'est pas par le prisme des droits et libertés individuels que la cybersécurité vient d'abord à l'esprit, et donc à l'agenda, mais par celui de l'intérêt des organismes, et plus précisément de leurs intérêts vitaux. La crainte de l'interruption d'activité, bien sûr, vient en premier. Suivent les risques d'atteinte au patrimoine informationnel, qu'il s'agisse de secrets d'État ou de secrets industriels et commerciaux, à protéger contre toute menace de chantage ou contre des menées d'intelligence économique. Rien de nouveau, jusqu'ici, à l'ère numérique. Et pourtant, depuis les années 2000, les bases de données personnelles ont pris une place accrue dans ce patrimoine informationnel. Terreau de l'économie numérique, particules élémentaires d'un grand nombre d'activités commerciales, elles sont devenues un actif stratégique de grande valeur.

C'est là que se rejoignent les droits des individus et les intérêts des organismes traitant la donnée. On pourrait n'y voir qu'une superposition accidentelle. Or, les deux sont intrinsèquement liés. Une violation de données affecte simultanément deux catégories de victimes : les personnes physiques et les organismes (privés ou publics). Du côté des personnes physiques, s'il s'agit d'une atteinte à la confidentialité de leurs données, elles risquent purement et simplement de voir leur vie privée divulguée ou menacée de l'être avec les risques qui s'ensuivent : chantage, tentatives d'hameçonnage, voire usurpation d'identité. L'impact psychologique associé est réel. S'il s'agit d'une atteinte à la disponibilité ou à l'intégrité de leurs données personnelles (quand les données sont confiées à des tiers comme lors de la disparition de photos téléchargées sur un service en ligne, la disparition d'un dossier médical également chargé en ligne), les personnes perdent là aussi, selon des degrés divers, une forme de maîtrise de leur vie privée, voire intime.

Du côté des organismes, une violation de données représente une atteinte à leur réputation mais aussi parfois une perte économique sèche. On pourra citer à titre d'exemple l'attaque de la banque du Bangladesh qui permit de dérober 101 millions de dollars. Aucun organisme ne peut rester absolument indemne face au préjudice d'image et de réputation causé par un incident de sécurité affectant la protection de ses données dès lors que cet incident reçoit une publicité. Et les faits rappellent régulièrement que conserver le secret sur un incident n'est ni souhaitable, ni parfois possible en pratique, ni d'ailleurs légal, dans certains cas de figure.

On l'a vu, l'organisme et les personnes physiques ne sont que les deux faces d'une même médaille. De même, il est assez vain de vouloir distinguer, dans une politique de sécurisation de son patrimoine, les données personnelles et celles qui sont des données « non personnelles ». L'imbrication est fréquente et justifie une dynamique commune.

Ce qui caractérise surtout l'évolution récente de notre économie numérique, c'est que cette imbrication est de plus en plus systémique. Un incident reste rarement cantonné au face-à-face entre un organisme et un individu : ce sont le plus souvent des fichiers, des bases entières, qui sont concernés. Une attaque peut toucher une masse d'individus se comptant en centaines, en milliers voire en millions. De manière plus générale, la combinaison de la quantité, de la précision, de la variété, de la richesse des données traitées (qu'il s'agisse des données collectées initialement, de celles générées par l'activité des individus en ligne ou des données inférées par les opérateurs) fait de la sécurisation de ce patrimoine une condition absolue de la confiance que les citoyens peuvent nourrir dans les fondements mêmes de l'économie numérique.

La cybersécurité est donc la clé de voûte de ces modèles économiques. Il en va de même pour les nouveaux modèles d'administrations publiques que l'on a vus se développer depuis les années 1990 sur l'exploitation d'un seul et même terreau : la donnée personnelle. Côté pile, on trouve le patrimoine informationnel constitué de ces données, combinées, enrichies, massifiées. Côté face, on doit trouver la confiance des personnes physiques dans la capacité des organismes à traiter leurs données conformément à leurs engagements, et, en tant qu'ils en sont les dépositaires, à ne pas les perdre. L'équation ne se simplifie guère lorsqu'on y ajoute les nombreuses forces centrifuges de notre économie numérique : transferts internationaux (d'un point A à un point B, mais aussi les transferts ultérieurs), multiples intermédiaires au sein de chaînes de sous-traitance ou de coresponsabilité parfois complexes et opaques, stockage dans le *cloud*, etc.

Le RGPD, un puissant outil de cybersécurité

La loi Informatique et Libertés du 6 janvier 1978 n'avait pas la réputation d'être un instrument de cybersécurité. Et pourtant, elle l'était au plus haut point. Dès 1978, son article 29 précisait que : « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. » Tout y était : l'obligation, sa définition, et sa raison d'être, à savoir la confiance mise par les déposants dans le dépositaire. Et de fait, la sécurité était déjà omniprésente dans les contrôles opérés par la CNIL et leurs suites répressives. Bon an, mal an, au moins 80 % des contrôles mettaient en lumière des manquements à l'obligation de sécurité, et une majorité des sanctions prises chaque année par la formation restreinte de la CNIL épinglaient des manquements de cette nature.

Cependant, force est de constater que la loi de 1978, avant-gardiste d'une certaine manière, n'a pas pu ou su créer l'électrochoc nécessaire pour rehausser le niveau de sécurité des organismes français, publics ou privés. S'inscrivant dans la continuité du texte français et en application depuis le 25 mai 2018, le Règlement général sur la Protection des Données (RGPD) doit désormais venir en concrétiser pleinement les promesses.

Le RGPD reprend, tout d'abord, l'obligation de sécurité. Sans en modifier en rien la substance, il en enrichit – et en allonge – la formulation. Sans entrer dans les détails, on peut mentionner le soin mis par l'article 32 à souligner la nécessaire adéquation et proportionnalité des mesures de sécurité à la nature et à l'intensité concrètes des risques dans chaque contexte ; la mention expresse du chiffrement dans la panoplie des mesures ; l'approche très large retenue de la notion de sécurité, incluant « la confidentialité, l'intégrité, la disponibilité et la résilience constantes » des systèmes d'information, etc. Rien dans cette approche n'est étranger à la doctrine d'emploi, par la CNIL, de la loi du 6 janvier 1978. Mais tout est désormais écrit, expressément.

Innovation apportée par le RGPD : le niveau des sanctions désormais applicables est considérablement rehaussé. À la hauteur des enjeux, les sanctions peuvent aller jusqu'à 2 % du

chiffre d'affaires mondial ou 10 millions d'euros pour un manquement à la sécurité – le plus élevé des deux plafonds étant retenu.

Le RGPD rend donc plus crédible l'obligation de sécurité préexistante. Par ailleurs, tenant compte des écosystèmes complexes de traitement des données, il met à la charge des sous-traitants des obligations propres – assorties de sanctions propres aux prestataires – en matière notamment de sécurité, alors que le droit antérieur ne connaissait qu'une seule tête : le responsable de traitement. Cela ne signifiait pas que le sous-traitant était déresponsabilisé avant le 25 mai 2018, mais sa responsabilité était avant tout contractuelle ou commerciale, par ricochet. Désormais, le contenu du contrat est spécifié à l'article 28 et le sous-traitant doit en outre répondre, devant le régulateur voire devant le juge, de ses obligations en matière de sécurité.

Mais la principale innovation du RGPD, propre au domaine de la cybersécurité, réside dans la mise en place de multiples procédures autour de l'obligation de sécurité, la mettant ainsi au cœur de la gouvernance et des process des organismes et créant d'utiles cordes de rappel pour les organismes qui la perdraient de vue.

On peut notamment citer le dispositif mis en place en cas de violation de données. À trois étages, ce dispositif va *crescendo* en fonction du degré de risque pour les droits des personnes. Si la violation n'entraîne pas de risque, le responsable du traitement doit seulement documenter, en interne sous forme d'un registre, la violation qui vient de se produire. Si elle entraîne un risque, il doit en outre notifier cette violation à la CNIL, au plus tôt et dans un délai en principe maximal de soixante-douze heures. Si la violation entraîne un risque élevé, il doit, enfin, informer les personnes concernées de la violation dont leurs données ont fait l'objet, au plus tôt. L'organisme peut différer cette information (à la différence de la notification à la CNIL) en cas de nécessité, liée par exemple à la mise en place d'une opération de cyberdéfense ou à l'ouverture d'une enquête sur l'origine et les canaux de l'attaque.

Cette nouvelle « discipline de la sécurité » monte progressivement en puissance. Au cours de la première année d'application du RGPD, la CNIL a reçu plus de 2 000 notifications de violation – pour environ 89 000 au niveau de l'Union européenne, avec de fortes variations d'un État à l'autre. Ce dispositif à trois étages a, en réalité, une triple vertu : faire monter en compétence les organismes sur les questions de cybersécurité en les incitant à mieux maîtriser leurs risques et à apprendre à réagir en cas d'incident ; protéger les personnes physiques concernées par une violation contre les risques subséquents (hameçonnage par exemple) ; intérioriser le caractère systémique des enjeux de sécurité qui lient l'entité et l'ensemble des personnes physiques embarquées dans ses traitements de données, et proportionner les obligations de l'une aux risques causés pour les autres.

Le RGPD prévoit une autre obligation procédurale en matière de sécurité : la réalisation, avant la mise en œuvre d'un traitement susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, d'une analyse d'impact relative à la protection des données. L'analyse d'impact est, fondamentalement, une analyse de risque évaluant de façon formalisée les impacts sur les personnes et sur les entreprises. Elle inclut un plan d'action en matière de sécurité et également un principe d'amélioration continue. De nouveau, l'obligation de procédure, de méthode, doit conduire à se poser les bonnes questions, à acquérir des réflexes, à trouver des solutions pour, au final, mieux protéger (et donc mieux traiter) les données personnelles des uns et des autres.

La cybersécurité et le RGPD, du texte à la politique publique

Un texte ne fait pas une politique publique. C'est en impulsant dans son domaine et en animant, aux côtés d'autres institutions, une véritable politique publique de cybersécurité que la CNIL entend traduire en actes les potentialités du RGPD – et contribuer à rehausser collectivement d'un

ou, si possible, de plusieurs crans le niveau de « cybersécurité collective » dans notre pays, tant le niveau de départ est, pour le dire pudiquement, perfectible.

Cela suppose, tout d'abord, de tenir un discours de cybersécurité accessible à tous les organismes, des plus petits aux plus gros. En matière de protection des données personnelles, l'expérience montre que c'est en embarquant tout l'écosystème économique et administratif que l'on peut efficacement limiter les points de fuite, tant ils sont nombreux. La cybersécurité doit donc se démocratiser, et toucher les petites et moyennes entreprises, les collectivités publiques de petite taille, ou encore le secteur associatif. La CNIL leur consacre des outils dédiés (guide PME-TPE élaboré avec la Banque publique d'Investissement, guide dédié à la sensibilisation des collectivités territoriales), en cohérence avec les contenus éditoriaux de l'ANSSI (qui a publié en partenariat avec la CPME un guide des bonnes pratiques de l'informatique). Elle cherche également de plus en plus à développer des contenus pédagogiques à leur attention (registre simplifié des opérations de traitements, etc.) Cette orientation doit se poursuivre dans les années à venir, possiblement sous de nouvelles formes (recommandations, règlements-types, etc.). La pédagogie ne passe pas seulement par le discours, mais aussi par des outils maniables, numériques, pour passer aux travaux pratiques. La CNIL a ainsi outillé ses guides « sécurité » et « AIPD » dans un logiciel gratuit et *open source*, disponible en dix-huit langues.

Mais cela suppose aussi de sensibiliser et de faire monter en compétence les citoyens eux-mêmes sur les sujets de cybersécurité. En effet, tout ne peut pas reposer sur les seuls organismes : les individus ont leur propre part de responsabilité. Sans verser dans un quelconque pessimisme, le caractère systémique des risques, à l'ère informationnelle, nécessite, très sérieusement et avec détermination, une mobilisation de tout le tissu social autour de cet enjeu commun. L'éducation au numérique sous toutes les facettes, c'est-à-dire l'éducation aux « dessous des cartes » de l'économie numérique, aux bonnes et mauvaises pratiques en ligne, et en particulier aux bons réflexes à adopter dans la sécurisation de sa vie privée (et de celle des autres) sur le web, fait partie intégrante de cette entreprise. Les « 10 conseils pour rester net sur le net », la réalisation d'une vidéo du Youtubeur *Le rire jaune* en partenariat avec la CNIL et la MGEN, et d'autres actions de la CNIL ou des membres du collectif Educnum, tendent à diffuser cette culture.

L'entrée en application du RGPD marque donc une étape essentielle dans le rehaussement du niveau de cybersécurité du pays et du continent européen. Il ne fera pas tout, loin de là. Mais au-delà des obligations connexes et des procédures qu'il a créées, le RGPD aura apporté sa pierre. Il jette les bases, en matière de cybersécurité, d'une politique publique. Il est temps de mesurer l'imbrication des enjeux pour les citoyens comme pour les organismes et d'être à la hauteur.