Actualités

Libres propos

529

La responsabilité de l'administration numérique sera-t-elle virtuelle ?

POINTS CLÉS ➤ Le développement des outils numériques et des bases de données par l'administration crée un risque certain ➤ À l'heure actuelle, les conditions d'engagement de la responsabilité de la puissance publique en cas de piratage apparaissent difficiles à satisfaire

Hicham Rassafi-Guibal,
docteur en droit public, chercheur, université du Luxembourg

On a beaucoup abordé la question de la (mauvaise) utilisation que pourraient faire les personnes publiques de fichiers informatiques (la violation d'un fichier par un agent de l'administration elle-même relève plutôt d'une violation des règles d'accès et d'utilisation de celui-ci. Elle est susceptible de constituer une faute justifiant sanction. Voir, pour une utilisation non autorisée du STIC : *CE, 31 mars 2017, n° 393216, Philippe Pichon : JurisData n° 2016-027949*), et les atteintes qu'ils portent, en eux-mêmes, aux droits et libertés fondamentaux (*C. Husson, Les droits de l'homme sont-ils solubles dans internet ? : JEDH, 2014-1, p. 29-53*). Déjà, la seule détention par l'État d'informations personnelles constitue, dans certaines circonstances, une ingérence dans le droit à la vie privée (*CEDH, 18 sept. 2014, n° 21010/10, Brunet c/ France : JurisData n° 2014-020611*).

Mais, le présent questionnement n'est pas tant relatif à l'usage – ou au mésusage – que pourrait faire l'État des données personnelles, qu'à l'accès et aux usages par des tiers non autorisés (*M. Bourgeois et A. Bounedjoum, Les apports de la loi pour une République numérique en matière d'accès et de réutilisation d'informations publiques : JCP A 2016, 2307*). En d'autres termes, il s'agit de s'intéresser aux conséquences juridiques d'un piratage informatique.

Le développement de l'administration numérique (*L. Cluzel-Metayer, La loi pour une République numérique : l'écosystème de la donnée saisi par le droit : AJDA 2017, p. 340*) conduit les personnes publiques à accumuler de plus en plus de données personnelles (parfois contre la volonté des personnes : V. pour le service public de l'éducation : *CAA Lyon, 3 mai 2016, n° 14LY00770*). Ainsi, l'obligation de télédéclaration fiscale (*CGI, art. 1649, quater et quinquies, 1681 septies et 1738*) amène les services de Bercy à disposer de très nombreuses informations sensibles. L'actualité récente démontre suffisamment l'intérêt de la question. Les vagues d'attaques informatiques de ces derniers mois (*en mai 2017 : Le Monde, 14 mai 2017, 200 000 victimes, 150 pays : le premier bilan de la cyberattaque mondiale, ainsi qu'en juin 2017 : Le Monde, 27 juin 2017, Le virus Petya paralyse entreprises et administrations à travers le monde*) ont eu des conséquences graves. Le cas le plus inquiétant s'est matérialisé dans la paralysie de certains hôpitaux britanniques à la suite d'une attaque par *ransomwares* (*ibid.*).

La responsabilité des personnes publiques pourrait-elle être engagée en cas d'attaque informatique paralysant des services publics ou permettant la collecte de données personnelles par piratage ?

Dans l'architecture actuelle du droit de la responsabilité de la puissance publique, deux causes sont invocables, mais aucune n'est totalement satisfaisante (les actions collectives sont inefficaces en matière de responsabilité : *L. n° 78-17, art. 43 ter, III*). La première est fondée sur la faute qui consisterait, pour les personnes publiques, à ne pas suffisamment organiser la protection des données (concernant la responsabilité pénale, le délit institué par l'article 226-17 du Code pénal est d'une efficacité limitée, compte tenu des conditions restrictives posées à l'article 121-2). La vulnérabilité du fichier TES (*G. Koubi, Le méga-fichier des titres électroniques sécurisés : JCP A 2016, 2300*) avait, de ce point de vue, conduit la rédaction des avis réservés du Conseil national du numérique (*CNN, Avis sur le fichier TES, déc. 2016*) et de l'ANSSI (*ANSSI et DINSIC, Audit du système « Titres électroniques sécurisé », 17 janv. 2017*). De même, la péremption des systèmes d'exploitation des administrations fait courir un risque important et pourrait constituer une faute (ce simple constat conduit à relancer l'appel à l'utilisation des logiciels et systèmes d'exploitation libres par l'administration, ne serait-ce que pour des raisons budgétaires). Mais l'administration ne serait tenue de réparer le préjudice qu'à concurrence des dommages causés par sa propre faute (*CE, 9 nov. 2016, n° 393902, 393926, Faure c/ Ministre des Affaires sociales : JurisData n° 2016-023458*).

La seconde cause mériterait une attention plus soutenue. On sait qu'en l'état actuel du droit positif, et indépendamment des divergences doctrinales, le risque et la rupture d'égalité devant les charges publiques sont susceptibles de fonder une responsabilité sans faute (*CE, 28 mars 1919, n° 62273, Regnault-Desroziers : Lebon 1919, p. 319*). La première hypothèse, notamment, semble dans son principe pouvoir fournir une solution à la présente problématique. En accumulant au sein de bases de données des informations sensibles, l'État et les personnes publiques créent un risque. Aucune mesure de sécurité informatique ne sera suffisamment efficace pour garantir l'inviolabilité des systèmes. Il n'en demeure pas moins que, sur le plan pratique, les conditions tenant au préjudice indemnisable, et notamment la condition de spécialité, risqueraient de n'être pas remplies dans le cas d'un vol massif de données. En revanche, la paralysie dommageable d'un service public pourrait, elle, voir satisfaite cette condition et ouvrir droit à indemnisation.

Si la responsabilité directe de la puissance publique ne pouvait être engagée, les hypothèses permettant l'indemnisation s'amenuiseraient (en contradiction avec le principe posé par l'article 82 du règlement *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : PE et Cons. UE, règl. (UE) 2016/679, 27 avr. 2016*). Ce n'est qu'en cas d'utilisation frauduleuse de données bancaires volées que la responsabilité de la banque pourrait être engagée sur le fondement de l'article L. 133-18 du Code monétaire et financier. Quant au fonds d'indemnisation des victimes d'infraction, il ne pourrait être mobilisé, le délit de violation de système informatisé (*C. pén., art. 323-3*) n'entrant pas dans son champ d'application (*CPP, art. 706-3*).