Nouvelles réponses à la cybercriminalité

Les différentes facettes criminelles de la sphère internet – contenus nocifs, escroqueries, cyberattaques, pédopornographie – appellent sans cesse de nouvelles réponses du législateur.

Elles se développent, classiquement, en termes d'extension ou de diversification des incriminations, d'aggravation des peines. Petit à petit, sont également conférés aux enquêteurs des outils plus adaptés à la recherche et à la conservation des preuves : infiltration numérique, gel de données informatiques, etc. Les nouvelles obligations des entreprises liées aux déclarations d'incidents, ou bien celles des fournisseurs d'accès et d'hébergement, constituent encore autant de ripostes.

Par-delà ce fourmillement, la politique de cybersécurité se dessine.

Cyberattaques : la lutte s'intensifie

par Emmanuel Daoud
Avocat à la Cour
et Géraldine Péronne
Docteur en droit, Avocat à la Cour

Les cyberattaques sont légion. La dernière en date a rendu publiques les données à caractère personnel de plus de 35 millions d'utilisateurs d'un site internet de rencontres extraconjugales[1].
Si l'opprobre ainsi jeté sur ces internautes par des hackeurs moralisateurs pourrait prêter à sourire, le nombre de personnes exposées et la récurrence des cyberattaques, dont une minorité seulement sont médiatisées, laisse pantois.
Le terme cyberattaque a lui-même engendré de multiples déclinaisons telles que cybermenace, cybersabotage, cyberagression, cyberhacktivisme, qui reflètent à la fois les craintes légitimes que le phénomène suscite[2], mais aussi la difficulté à cerner les contours de celui-ci.
Ce dernier point peut s'expliquer par le caractère relativement récent de la problématique des cyberattaques. L'un des premiers virus, le «ver Morris» (*Morris worm*) lancé en 1988 par un étudiant américain, peut être considéré comme la première forme d'attaque informatique diffusée par internet. Initialement conçu aux fins de déterminer la taille du réseau, le virus échappe finalement à son auteur et se propage rapidement, paralysant des milliers d'ordinateurs.
Les cyberattaques se multiplient véritablement à partir du milieu des années 2000, à un moment où internet est accessible à tous, où les entreprises et administrations dématérialisent les procédures et disposent toutes d'un site internet.
Ce constat initial conduit à s'interroger sur l'aspect essentiellement factuel auquel est souvent réduit le phénomène des cyberattaques, englobé dans le concept plus large de cybercriminalité. La tentation est grande de vouloir en dresser une typologie. Les cyberattaques, par essence très variées, se différencient tant par leur modes opératoires que par l'identité de leur cible ou encore la nature des objectifs poursuivis. Ne pourrait-on pas ainsi élaborer trois catégories : les cyberattaques à visée revendicatrice, les cyberattaques mercantiles et les cyberattaques aux fins d'espionnage ?
Les premières revendiquent des opinions politiques, religieuses ou des idées terroristes[3] ou cherchent simplement à démontrer une supériorité technique en décelant et en dénonçant des failles dans un système informatique. La cyberattaque de nature terroriste dont a été victime la chaîne de télévision française TV5 Monde en avril dernier s'inscrirait dans cette catégorie.
Les secondes se rapporteraient à la collecte de données relatives à un secret industriel en vue d'une exploitation lucrative ou de données à caractère personnel en vue d'une revente sur un marché parallèle.
Le troisième type de cyberattaques serait relatif aux attaques diligentées par des agents des services de renseignement d'un pays à l'encontre de systèmes d'information étrangers en vue d'un espionnage de nature économique ou aux fins de collecte d'informations relatives à la sécurité nationale[4]. Les États-Unis ont récemment soupçonné la Chine d'être à l'origine de deux attaques en avril et en juin dernier ayant permis le vol de données personnelles de 21,5 millions de personnes sur des bases de données gérées par le gouvernement américain[5].
Néanmoins, de telles classifications ne peuvent servir qu'un objectif de meilleure compréhension des attaques et de leur diversité, les frontières entre les catégories étant assez poreuses. Depuis la loi Godfrain du 5 janvier 1988 relative à la fraude informatique[6] qui a introduit des dispositions spécifiques dans le code pénal, le législateur propose une distinction autre, portant sur les différents modes d'atteinte à un système de traitement automatisé de données (STAD) : accès et maintien frauduleux (C. pén., art. 323-1), entrave au fonctionnement du système (art. 323-2) et introduction frauduleuse de données (art. 323-3).
La question est donc moins celle de savoir si une classification est possible que de s'assurer que le droit positif répond de manière adéquate à l'intensification des cyberattaques.
L'analyse des textes et de la jurisprudence met en évidence un mouvement progressif de renforcement des incriminations pénales, tandis que les obligations administratives pesant sur le maître du système de traitement de données s'accroissent, dans un effort conjugué de répression des cyberattaques et d'encadrement de leurs effets.

Le renforcement des incriminations pénales

Le renforcement des incriminations pénales d'atteintes à un système de traitement automatisé de données se traduit en premier lieu par une portée élargie des infractions, et en second lieu par l'aggravation des sanctions.

L'élargissement de la portée des infractions

Évoquer un élargissement de la portée des infractions pourrait surprendre tant il semble de prime abord que ces infractions couvrent d'ores et déjà un champ d'ap-

(1) Piratage: derrière Ashley Madison, un groupe à la réputation sulfureuse, *Le Monde*, 19 août 2015.
(2) Une enquête a révélé que 89 % des citoyens de l'Union européenne évitaient de divulguer des données à caractère personnel en ligne et que 74 % d'entre eux pensaient que le risque d'être victime d'un acte de cybercriminalité avait augmenté (A. Astaix, Cybercriminalité: les citoyens de l'Union se préoccupent de la sécurité des données, Dalloz actualité, 13 juill. 2012).
(3) Ces cyberattaques pourraient être qualifiées d'actes terroristes au sens de l'art. 421-1, 2°, C. pén. M. Quéméner, Le terrorisme face au cyberespace, de l'anticipation des risques à la répression, AJ pénal 2013. 446.
(4) Cette hypothèse a récemment reçu une consécration législative par le biais de la L. n° 2015-912 du 24 juillet 2015 sur le renseignement introduisant un nouv. art. 323-8 au sein du code pénal. Cette disposition prévoit que les agents des services spécialisés de renseignement peuvent porter atteinte à des systèmes de traitement automatisé de données «pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'art. L. 811-3 [code de la sécurité intérieure]».
(5) Hacking of Government Computers Exposed 21,5 Million People, *The New York Times*, 9 juill. 2015.
(6) L. n° 88-19 du 5 janv. 1988 relative à la fraude informatique, JO 6 janv.

plication vaste. Cette impression repose notamment sur l'acception large du support des infractions : le système de traitement automatisé de données.
La loi ne définissant pas cette notion[7], la jurisprudence a pu considérer que les terminaux de paiement par carte bancaire constituaient de tels systèmes[8]. Elle pourrait y assimiler également les systèmes de téléphonie type PABX, qui s'apparentent à de véritables serveurs informatiques et dont le piratage est aujourd'hui fréquent. Les perspectives d'élargissement sont encore très grandes au regard du pullulement actuel des outils technologiques communément appelés « objets connectés ». Leur statut juridique n'est pas encore clairement établi, mais ils pourraient s'insérer dans cette catégorie, sans parler des développements à venir en raison de l'interconnexion de ces objets.
Outre ces interprétations jurisprudentielles potentielles, le législateur a expressément élargi le champ d'application de l'article 323-3 du code pénal.
La loi n° 2014-1353 du 13 novembre 2014 a modifié cette disposition afin d'y intégrer une nouvelle infraction. Il est ainsi prévu que : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».
Les termes « extraire, détenir, reproduire, transmettre » ont été ajoutés à la nouvelle version du texte de manière à fournir une base juridique claire au vol de données, un temps sanctionné par l'abus de confiance[9] ou l'infraction de vol de droit commun[10].
L'article 323-3 du code pénal suscite néanmoins quelques questions[11].
Il est ainsi possible de s'interroger sur le point de savoir si les faits réprimés, pris indépendamment, peuvent caractériser une infraction à eux seuls ou s'il convient de prouver un accès au système de traitement de données préalable (C. pén., art. 323-1). L'intrusion dans un système de données n'est-elle pas en effet une condition nécessaire à l'extraction de données, notamment ?
Il semblerait que l'article 323-3 soit doté d'une réelle autonomie. En effet, il ne renvoie pas formellement à l'article 323-1. De plus, quand le législateur a souhaité lier l'intrusion frauduleuse et la suppression ou la modification subséquente des données contenues dans le système, il l'a expressément prévu (C. pén., art. 323-1 al. 2). Il semble donc que même d'un point de vue substantiel, les articles 323-3 et 323-1 soient parfaitement indépendants.
Cela signifie donc que l'extraction peut être sanctionnée quand bien même l'accès au système de traitement automatisé de données aurait été licite, ce qui facilite la caractérisation de la première infraction.
Cette interprétation semble corroborée par la jurisprudence relative à l'article 323-1 du code pénal, qui a également étendu la portée de cette disposition.
L'article 323-1, alinéa 1er, prévoit en effet que « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. [...] ».
La jurisprudence a eu l'occasion de préciser, d'une part, que l'accès frauduleux supposait l'existence d'un système sécurisé dans un célèbre arrêt *Tati*[12] et d'autre part, que la caractérisation du maintien frauduleux ne reposait pas sur la démonstration d'un accès frauduleux.
Cette dernière solution a fait l'objet d'une réaffirmation récente dans un arrêt de la Chambre criminelle du 20 mai 2015. Une personne s'était introduite dans l'extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) et était parvenue à récupérer des documents dont l'accès n'était pas protégé. Les informations ainsi obtenues lui avaient permis de rédiger et de publier un article dans une revue scientifique[13].

Ne pourrait-on pas ainsi élaborer trois catégories : les cyberattaques à visée revendicatrice, les cyberattaques mercantiles et les cyberattaques aux fins d'espionnage ?

L'infraction d'accès frauduleux n'a pas été retenue par la Chambre criminelle car l'accès avait été rendu possible grâce à une défaillance du système. La solution est en cela conforme à la jurisprudence *Tati* qui requérait l'existence d'un système sécurisé pour caractériser l'accès frauduleux.
En revanche, l'autonomie de l'infraction de maintien frauduleux peut surprendre. Il paraît en effet difficile de concilier un maintien frauduleux dans un système avec un accès licite à celui-ci. Pourtant, la lettre du texte permet une telle dissociation par la conjonction « ou » qui distingue l'accès du maintien dans le système. La difficulté réside finalement dans la démonstration du caractère intentionnel du maintien, selon que l'individu avait conscience, ou non, de s'introduire frauduleusement dans un système.
La Chambre criminelle résout cette équation en considérant que cette intention était caractérisée dès lors que l'individu avait découvert que le système était protégé et s'y était toutefois maintenu[14].
En dépit des interrogations ou imprécisions qui peuvent subsister quant à l'interprétation des textes, la tendance de fond est donc celle d'un élargissement de la portée des infractions et subséquemment, d'un durcissement de la répression.

L'aggravation des sanctions

Conscients de la multiplication des cyberattaques et des enjeux de sécurité qui imprègnent ce phénomène, la volonté politique s'inscrit dans une démarche répressive qui transparaît encore dans une récente aggravation des peines pour les infractions prévues aux articles 323-1 et suivants du code pénal.

7) En revanche, on observera qu'un arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire informatique précise ce qu'il faut entendre par « système de traitement automatisé de données » : il s'agit de « l'ensemble des opérations réalisées par des moyens automatiques, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation ».
8) TGI Paris, 25 févr. 2000, D. Affaires 2000. 219, obs. X. Delpech.
9) Crim. 22 oct. 2014, n° 13-82.630, D. 2015. 415, note A. Mendoza-Caminade; CCE 2015. Comm. 17, note E. A. Caprioli.
10) Crim. 20 mai 2015, n° 14-81.336, D. 2015. 1466, note L. Saenko; Lamyline actualité, 5 juin 2015, obs. C. Duhil de Bénazé; AJ pénal 2015. 393, note E. Dreyer (*infra*).
11) Saisie d'une question prioritaire de constitutionnalité portant sur la légalité de l'art. 323-3, C. pén., la Cour de cassation a décidé que les termes de la disposition étaient « suffisamment clairs et précis pour que son interprétation et sa sanction, qui entrent dans l'office du juge pénal, puissent se faire sans risque d'arbitraire », Crim. 10 avr. 2013, n° 12-85.618, RSC 2013. 559, chron. J. Francillon.
12) Il ne peut « être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties d'un site qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties du site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être présumées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès », Paris, 30 oct. 2002, C. Morel, Pas d'accès frauduleux sans sécurité, Expertises, janv. 2003.
13) Crim. 20 mai 2015, n° 14-81.336, *op. cit.* note 10.
14) V. égal. Crim. 3 oct. 2007, n° 07-81.045, AJ pénal 2007. 535, obs. Royer; D. 2007. 2807; RSC 2008. 99, obs. J. Francillon; RTD com. 2008. 433, obs. B. Bouloc.

Depuis l'entrée en vigueur de la loi n° 2015-912 du 24 juillet 2015 sur le renseignement, les amendes sanctionnant les infractions commises à l'encontre de systèmes de traitement de données ont ainsi doublé ou triplé selon les cas. Ainsi, par exemple, le montant de l'amende pour l'accès ou le maintien dans un STAD est passé de 30 000 euros à 60 000 euros (art. 323-1, al. 1er) ; celui de l'amende encourue pour le fait d'entraver ou fausser un STAD mis en œuvre par l'État est passé de 100 000 euros à 300 000 euros (art. 323-2, al. 2)[15]. L'arsenal coercitif et dissuasif ainsi mis en œuvre se heurte néanmoins à deux obstacles non négligeables. Le premier tient à la difficulté d'identifier les auteurs des infractions, ceux-ci se dissimulant derrière des dispositifs techniques très complexes qui favorisent leur anonymat. Le second tient aux effectifs encore trop réduits des brigades spécialisées telles que la Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), confrontées à une charge de travail croissante et à des infractions d'une grande sophistication. On notera néanmoins la création d'un cyber-préfet chargé de coordonner la lutte contre les cyberattaques visant les petites et moyennes entreprises, dont l'avenir est prometteur[16].

Les opérateurs de télécommunication, la SNCF ou encore EDF, sont aujourd'hui contraints de déclarer tout incident de sécurité à l'ANSSI.

À cette répression pénale renforcée s'ajoutent des obligations administratives toujours plus étendues permettant aux autorités régulatrices compétentes de surveiller et d'encadrer les effets des cyberattaques.

L'extension des obligations administratives

Outre le juge pénal, deux autres acteurs participent de la lutte contre les cyberattaques : l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la Commission nationale pour l'informatique et les libertés (CNIL). Ces deux autorités intensifient progressivement leur contrôle en obligeant certains opérateurs à déclarer les incidents de sécurité d'une part et à notifier toute violation de données personnelles d'autre part.

L'obligation de déclaration d'un incident de sécurité

La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire a introduit dans le code de la défense de nouvelles dispositions en matière de sécurité des systèmes d'information (art. L. 1332-6-1 à L. 1332-6-6). Un décret en Conseil d'État précisant concrètement les modalités d'application de ces articles est entré en vigueur le 30 mars 2015[17].

L'objectif des dispositions précitées du code de la défense est d'organiser la protection des « installations d'importance vitale ». L'article L. 1332-1 de ce même code définit ainsi « l'opérateur d'importance vitale » (OIV). Il s'agit des « opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation [...] ».

À l'aune de ces nouvelles dispositions, les opérateurs de télécommunication, la SNCF ou encore EDF, sont aujourd'hui contraints de déclarer tout incident de sécurité à l'ANSSI, qui voit ainsi ses pouvoirs de surveillance élargis.

Cette nouvelle obligation fait écho au principe existant de notification à la CNIL d'une violation de données à caractère personnel.

L'obligation de notification de violation de données personnelles

Les cyberattaques et le droit des données personnelles sont intimement liés, tant il est fréquent que le piratage informatique porte atteinte à des données à caractère personnel.

Conformément à l'article 34 *bis* de la loi n° 78-17 du 6 janvier 1978 modifiée, les fournisseurs de services de communications électroniques au public, tels que définis par l'article L. 33-1 du code des postes et des communications électroniques, ont l'obligation de notifier à la CNIL les violations de données à caractère personnel. En l'état du droit positif, aucune notification de ces violations n'est obligatoire pour les autres opérateurs économiques. De même, ceux-ci ne sont pas dans l'obligation d'informer les personnes concernées de l'atteinte portée à leurs données personnelles.

Cela pourrait changer avec l'entrée en vigueur prochaine du règlement européen sur la protection des données à caractère personnel. En effet, le G29, qui regroupe l'ensemble des CNIL européennes, a publié un avis récent sur le texte européen, par lequel il indique qu'il est essentiel de fournir des garanties afin de s'assurer que les violations de données ne sont pas dissimulées, que l'évaluation de la violation est menée correctement et que les personnes concernées reçoivent notification chaque fois que cela est requis[18]. Il y a fort à parier que le futur règlement intégrera cette volonté générale de transparence dont seules les modalités restent encore à déterminer.

L'étau se resserre sur les auteurs des cyberattaques tandis que les opérateurs économiques victimes sont de plus en plus souvent contraints de rendre des comptes. C'est sans nul doute le prix à payer pour une plus grande efficacité de la répression.

(15) V. tous les nouveaux montants des amendes encourues aux art. 323-1, 323-2 et 323-3.

(16) Annoncés en juin 2014 par B. Cazeneuve, les premiers cyber-préfets ont été nommés il y a quelques mois.

(17) Décr. n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, C. défense, art. R. 1332-41-1 et s.

(18) Avis du G29 du 17 juin 2015 (traduction libre de l'anglais), p. 16 (disponible sur le site Internet de la CNIL).