La cybercriminalité à l'ère de la crise sanitaire

Hélène Christodoulou

La cybercriminalité à l'ère de la crise sanitaire

Hélène Christodoulou
Docteur qualifié en droit privé, UT1

La cybercriminalité à l'ère de la crise sanitaire

Hélène Christodoulou
Docteur qualifié en droit privé, UT1

La crise sanitaire liée au Coronavirus a des incidences mondiales plurielles. La recrudescence de la cybercriminalité commise à l'aide de modes opératoires connus, dans un contexte quant à lui inédit, en est une illustration dont il s'agira de brosser le portrait.

À l'ère de la « guerre sanitaire »[1], la guerre numérique semble, également, déclarée. Cette dernière apparaît même plus dangereuse « pour la stabilité des démocraties et des économies que les fusils et les chars »[2]. Nombreux sont les internautes qui reçoivent, via une adresse mail fictive d'une autorité de santé, des courriels relatifs au Covid-19 infectés par des virus ou encore qui pensent acheter des produits d'hygiène au travers d'un faux site internet. En somme, la commission de cyberattaques ne cesse d'abonder dans un contexte sans précédent.

La « cybercriminalité », « la criminalité dans le cyberespace », le « cybercrime », « les infractions liées à la criminalité informatique » ou « à la haute technologie » sont des notions interchangeables[3], aux contours insaisissables, tant elles demeurent par essence polymorphes et mouvantes[4]. Concrètement, la cybercriminalité apparaît comme une nébuleuse faisant écho à des infractions commises, au sein du cyberespace, à l'aide de « procédés techniques essentiellement évolutifs maîtrisés par les seuls initiés »[5]. Partant, « il est très difficile d'en tirer quelque conclusion que ce soit, tant les enjeux, les acteurs et les dynamiques à l'œuvre sont divers et hétéroclites »[6]. Pour autant, la Convention de Budapest[7], reprise en des termes semblables par la Commission européenne[8], tente d'y apporter une

[1] Le mot « guerre » ayant été prononcé sept fois, Macron E., « Discours du Président de la République française relatif au Covid-19 », 16 mars 2020, 20h.

[2] Juncker J.-C., « Discours sur l'état de l'Union », 13 sept. 2017.

[3] V. sur ce point, Conseil de l'Europe, Convention sur la cybercriminalité, Budapest, 23 nov. 2001 ; Commission européenne, Communication, « Vers une politique générale en matière de lutte contre la cybercriminalité », MEMO/07/199, 22 mai 2007.

[4] V. sur ce point Chopin F., « Cybercriminalité », Rép. pén. Dalloz 2020 ; Quemener M., « La justice face au défi de la cybercriminalité : constat et préconisation », Conseil de l'Europe 2019, Entretien 10, n° 12.

[5] Groupe de travail interministériel sur la lutte contre la cybercriminalité, « Protéger les internautes – Rapport sur la cybercriminalité », févr. 2014, p. 9.

[6] Rapport du centre international pour la prévention de la criminalité, *Prévention de la criminalité et sécurité quotidienne : prévenir la cybercriminalité*, 6e éd., 2018, p. 75.

[7] Conseil de l'Europe, Convention sur la cybercriminalité, Budapest, 23 nov. 2001.

[8] Communication de la Commission européenne, « Vers une politique générale en matière de lutte contre la cybercriminalité », MEMO/07/199, 22 mai 2007 ; V. sur ce point, Berthelet P., « La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas

définition opérationnelle, en visant deux catégories d'infractions au sein desquelles le système informatique apparaît central. Ce dernier peut en être soit la finalité, en ce que les infractions commises lui portent nécessairement atteinte[9] ; soit le moyen, en ce qu'elles sont réalisées grâce à lui[10]. À l'aune de cette définition, l'ensemble des législations nationales dispose donc d'un éventail d'infractions relevant de la criminalité informatique, mais des efforts quant à la convergence des droits internes sont encore attendus[11].

« La surface d'attaque »[12] de la cybercriminalité ne cesse de croître à mesure que les espaces et les objets numériques s'imposent dans le quotidien des populations[13]. En agissant contre ou en exploitant un système informatique, la commission de l'infraction apparaît aisée. Par un simple clic, « même si la mise en scène et les techniques utilisées sont souvent très élaborées »[14], il est possible d'attaquer simultanément plusieurs cibles dans le monde en profitant de l'anonymat et de la rapidité des transferts de flux offerts par la technologie afin de contourner les frontières physiques pour se perdre dans les méandres des réseaux.

Le caractère inédit des circonstances liées à la crise sanitaire mondiale a notamment permis l'ouverture d'une faille numérique au sein de laquelle les cybercriminels s'engouffrent à une vitesse fulgurante. Ainsi comment utilisent-ils la pandémie pour commettre des « cyber-infractions » tout aussi destructrices ?

Depuis le mois de mars, la presse ne cesse de relayer quotidiennement de nouvelles cyberattaques, commises à travers le monde, qu'il est difficile d'endiguer une fois consommées. Il s'agira alors de décrypter ce phénomène en dressant un constat relatif à la commission exponentielle de cette catégorie d'infractions à l'aide de modes opératoires connus par les autorités répressives (**II**), dans un contexte inédit (**I**).

institutionnels », RQDI 2018 vol. 2 (Hors-série) ; Berthelet P., « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne », RSC 2018, p. 59 et s.

[9] Les infractions sont visées au sein du titre 1 de la Convention de Budapest : l'accès illégal (art. 2), l'interception illégale (art. 3), l'atteinte à l'intégrité des données (art. 4), l'atteinte à l'intégrité du système (art. 5), abus de dispositif (art. 6).

[10] Les infractions sont visées au sein du titre 2 : la falsification informatique (art. 7), la fraude informatique (art. 8) ; au sein du titre 3 : la pornographie enfantine (art. 9) et au sein du titre 4 concernant les infractions liées à la propriété intellectuelle et aux droits connexes.

[11] Rapport du ministère de l'Intérieur, « État de la menace liée au numérique en 2019 », mai 2019, rapp. n° 3, p. 10.

[12] Rapport du ministère de l'Intérieur, « État de la menace liée au numérique en 2019 », mai 2019, rapp. n° 3, p. 18 et p. 128.

[13] Concrètement, le taux de pénétration de l'Internet progresse continuellement à hauteur de 88 % en France et de 55 % pourcents dans le monde, Rapport du ministère de l'Intérieur, « État de la menace liée au numérique en 2019 », mai 2019, rapp. n° 3, p. 13.

[14] Groupe de travail interministériel sur la lutte contre la cybercriminalité, « Protéger les internautes – Rapport sur la cybercriminalité », févr. 2014, p. 10.

I. – Un contexte inédit favorisant les cyberattaques

« Il existe des conditions structurelles et sociétales qui semblent liées à la cybercriminalité, tout comme des environnements propices à la commission de cybercrimes »[15]. Les émotions exacerbées des populations et l'usage intensif d'internet se cumulent de manière inouïe au bénéfice des cybercriminels qui n'ont pas manqué de saisir les opportunités offertes par ce nouveau contexte pour agir.

« Virtualité du symptôme, virtualité de l'angoisse, de la panique… Incertitude de la temporalité et de la localisation, incertitude de la spécificité du mode symptomatique… Ce qui se propage se manifeste de manière multiforme »[16]. Les doutes scientifiques concernant le virus et les mesures drastiques prises par les gouvernements, alimentés par les médias[17], mettent à rude épreuve l'émoi des populations. Ces dernières sont obnubilées par le seul fait de maîtriser « cette agression par la violence d'un virus qui circule sans être aperçu, diffus, caché, inconsistant et dont on ne peut que douter de sa présence dans le corps ? »[18]. Ainsi, la peur collective face à l'inconnu et *in fine* à la mort[19], mais aussi l'empathie, semblent se cristalliser autour du Covid-19. Il en découle une plus grande volonté de s'informer, de se procurer des objets hygiéniques voire d'aider autrui à distance, par le biais d'internet, comme le souligne le gouvernement français[20]. Or ces émotions ont pour effet de neutraliser l'esprit critique[21], constituant alors une situation favorable pour les cybercriminels maniant brillamment « l'ingénierie sociale »[22]. Si la propagation d'un virus n'est pas un phénomène nouveau[23], il le devient en étant cumulé avec les mesures de confinement prises par la plupart des gouvernements des plus grandes puissances mondiales.

« Le nombre d'internautes par habitant dans un pays influence grandement les taux de cybercriminalité de cette nation, que l'activité cybercriminelle en question soit l'objet d'actes commis par des délinquants résidant au sein du pays ou qui utilisent simplement cette nation comme un canal

---

[15] Kigerl A., « Mettre fin au processus de l'émergence de la cybercriminalité : des délinquants motivés aux cyberattaques », *in Rapport du centre international pour la prévention de la criminalité, Prévention de la criminalité et sécurité quotidienne : prévenir la cybercriminalité*, 6e éd., 2018, p. 77.

[16] Jeudy H.-P., *La peur et les médias – Essai sur la virulence*, 1979, PUF, p. 80.

[17] ~~I~~Jeudy H.-P., *La peur et les médias – Essai sur la virulence*, 1979, PUF, p. 80.

[18] À propos de la rage, Jeudy H.-P., *La peur et les médias – Essai sur la virulence*, 1979, PUF, p. 78.

[19] André C., « Éloge et usage de la peur au temps du coronavirus », *Libération*, 27 mars 2020.

[20] Article du gouvernement, « Recommandations de sécurité informatique pour le télétravail en situation de crise », 23 mars 2020.

[21] Barbezat E., « Coronavirus : la peur se propage encore plus vite que l'épidémie », *L'humanité*, 17 mars 2020.

[22] « L'ingénierie sociale fait référence à des pratiques de manipulation psychologique à des fins illicites. Ces pratiques exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre, par une mise en confiance, d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou à un système informatique, la divulgation d'informations…) », Rapport du ministère de l'Intérieur, « État de la menace liée au numérique en 2019 », mai 2019, rapp. n° 3, p. 45.

[23] Pour en savoir plus sur l'histoire des virus, v. Gessain A. et Manuguerra J.-C., *Les virus émergents*, 2006, PUF.

pour commettre leurs attaques »[24]. Par conséquent, le télétravail ne fait qu'accentuer ce phénomène, d'autant que sa mise en œuvre s'est faite dans l'urgence et à distance voire a dû dépendre des équipements personnels des collaborateurs « dont le niveau de sécurité ne peut pas être évalué et encore moins garanti »[25]. Ce contexte a, une nouvelle fois, favorisé les agissements des cybercriminels qui usent, néanmoins, de modes opératoires déjà connus par les autorités.

II. – Des modes opératoires connus favorisant les cyberattaques

Au regard du caractère transnational de la cybercriminalité, lié à l'essence dématérialisée des réseaux, des efforts d'harmonisation ont été constatés en Europe[26], même s'ils semblent encore insuffisants. En droit interne cette catégorie d'infractions illustre la « parcellisation de l'outil pénal »[27]. L'ensemble des normes est diffuse au sein du Code pénal et en dehors, faisant appel à des infractions spécifiques ou de droit commun[28], déstabilisant corrélativement le principe de la légalité pénale. Concrètement, les cyberattaques supposent la mise en œuvre d'une pluralité de modes opératoires[29] destinés majoritairement à « tromper » ou encore à « déstabiliser » des internautes, allant du simple particulier jusqu'à l'État en passant par les entreprises[30]. Dans le contexte du coronavirus, ces derniers sont ceux utilisés classiquement, mais de manière exponentielle.

D'une part, s'agissant des infractions commises contre le système informatique, il est possible de relever l'usage d'un « rançongiciel », autrement appelé « *ransonwares* ». Il s'agit d'un chantage effectué par la rétention volontaire des données de l'utilisateur, dans son cadre personnel ou professionnel, après l'avoir piégé en l'incitant à cliquer sur un lien porteur d'un virus. Ce dernier ne

---

[24] Kigerl A., « Mettre fin au processus de l'émergence de la cybercriminalité : des délinquants motivés aux cyberattaques », *in Rapport du centre international pour la prévention de la criminalité, Prévention de la criminalité et sécurité quotidienne : prévenir la cybercriminalité*, 6e éd., 2018, p. 78 ; Kigerl A., « Routine Activity Theory and the Déterminants of High Cybercrime Countries », Social Science Computer Review 2012, p. 304 et s.

[25] Article du gouvernement, « Recommandations de sécurité informatique pour le télétravail en situation de crise », 23 mars 2020.

[26] Conseil de l'Europe, Convention sur la cybercriminalité, Budapest, 23 nov. 2001 ; Berthelet P., « La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels », RQDI 2018 vol. 2 (Hors-série) ; Berthelet P., « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne », RSC 2018, p. 59 et s.

[27] Pereira B., « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », RIDE 2016, p. 395.

[28] Pereira B., « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », RIDE 2016, p. 395.

[29] Comme l'affirme Cabon S.-M. : « dans la pratique, la cybercriminalité renvoie moins à une liste d'infractions bien déterminées qu'à une manière d'opérer », v. Cabon S.-M., « L'influence du cyber espace sur la criminalité économique et financière », Dr. pén. 2018, étude 12.

[30] Doutriaux C., « Réponses des États pour prévenir la cybercriminalité ? », *in* Rapport du centre international pour la prévention de la criminalité, *Prévention de la criminalité et sécurité quotidienne : prévenir la cybercriminalité*, 6e éd., 2018, p. 135.

pourra récupérer ses données qu'à l'aide d'un code obtenu par le paiement d'une rançon au cybercriminel[31]. Actuellement, les victimes sont donc encouragées, au moyen de courriels, à cliquer sur un lien afin de découvrir le « remède miracle » pour guérir de la maladie ou encore à télécharger une application permettant de détecter la présence du virus sur soi ou son entourage[32]. En outre, l'attaque par déni de service retient, également, l'attention[33]. Cette dernière vise à noyer les serveurs informatiques sous de fausses requêtes jusqu'à les saturer, provoquant une dégradation voire une panne. À cet égard, les hôpitaux de Paris ou encore l'Organisation mondiale de la santé ont récemment subi ce type d'attaques[34], alimentant une nouvelle crise dans la crise.

D'autre part, s'agissant des infractions commises à l'aide d'un système informatique, les illustrations apparaissent plus abondantes. En mars 2020, par rapport au mois précédent, une hausse de 667 % du nombre « d'hameçonnage », autrement appelé « *phishing* », dans le monde a été constatée[35]. Cette technique a pour finalité de dérober des informations professionnelles, voire personnelles, en se faisant passer pour un tiers de confiance dans le but d'usurper l'identité de la victime[36]. À titre d'illustration, un site a pris l'identité d'une célèbre plateforme de *streaming* américaine afin de laisser croire aux internautes confinés qu'un accès gratuit leur était offert dans le but unique de récupérer leurs données[37].

De surcroît, ces derniers réalisent des « cyberescroqueries » qui supposent au travers d'un système informatique, « soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers »[38], à remettre dans la plupart des cas des fonds. Il s'agit ici d'une infraction de droit commun, l'escroquerie, appliquée à la cybercriminalité. Les auteurs réalisent de façon massive cette infraction au travers de modes opératoires variés. Ces derniers jours, des sites frauduleux sont créés afin de proposer divers produits

---

[31] Ce comportement est incriminé en France par les articles 323-1 et s. du CP portant sur les « atteintes aux systèmes de traitement automatisé des données ».

[32] Bayard F., « Coronavirus : des pirates profitent de l'épidémie pour propager de dangereux *malwares* », *Phonandroid*, 17 mars 2020 ; Paquette E., « Le coronavirus, une aubaine pour les cybercriminels », *L'express*, 22 mars 2020.

[33] *DDoS* pour *Distributed Denial of Service*, incriminé en France par les articles 323-1 et s. du Code pénal.

[34] Bastien L., « Covid-19 : Les cyberattaques contre l'OMS ont doublé depuis le début de la pandémie », Le big data, 25 mars 2020.

[35] Fleming S., « Threat Spotlight : coronavirus related phishing », Barracuda Networks, 26 mars 2020 ; Filippone D., « Avec le coronavirus, le *pishing* augmente de 667 % en mars », Le monde, 27 mars 2020 ; Vergelis M., « Attaque de phishing et coronavirus », Kaspersky, 7 févr. 2020.

[36] Ce comportement est incriminé en France par l'article 313-1 du Code pénal, relatif à l'escroquerie et par l'article 226-4-1 du Code pénal, relatif à l'usurpation d'identité.

[37] Dourdelles M., « Coronavirus – Netflix, nouvel appât d'une tentative de *phishing* », Que choisir, 27 mars 2020.

[38] Ce comportement est incriminé en droit interne à l'article 313-1 du Code pénal.

d'hygiène, constituant des denrées rares, comme les masques[39]. Dans le même temps, des escroqueries aux faux ordres de virement, dites « au président » ou « au changement de coordonnées bancaires », sont réalisées. Elles ont pour but d'inciter des sociétés à transférer des fonds de manière injustifiée au bénéfice d'usurpateurs. À cet égard, une entreprise pharmaceutique française a effectué une commande massive de masques et de flacons de gels hydroalcooliques en pensant le faire auprès de son fournisseur habituel, mais celle-ci s'est avérée être une société fantôme[40]. Au-delà de jouer sur la peur, les cybercriminels savent susciter l'empathie des internautes pour les escroquer en créant de fausses cagnottes en ligne dans le but d'aider les soignants, les hôpitaux ou encore les populations les plus fragiles durant la pandémie. Or les dons sont en réalité récoltés dans un but bien moins vertueux[41].

Enfin, un dernier exemple permet d'illustrer la recrudescence des cyberattaques par la circulation d'informations sur le coronavirus, fausses, inexactes ou trompeuses[42] « qui sont fabriquées, présentées et diffusées dans un but lucratif ou de manière à causer intentionnellement un préjudice public »[43]. Ainsi, une vidéo de « cadavres », jonchant les rues en Chine, présentés à tort comme des victimes de la pandémie, a circulé sur internet parmi tant d'autres pour affoler la population mondiale, alors qu'il s'agissait d'individus contraints de dormir dehors.

Afin de stopper ce phénomène polymorphe, les institutions nationales[44], européennes[45] et plus largement internationales[46] favorisent la prévention des internautes[47], plutôt que la répression des cybercriminels qui demeurent insaisissables, malgré la mise en œuvre d'une coopération pénale, encore en construction, entre les États[48]. Ainsi, en intervenant antérieurement à la commission de

---

[39] Piel S. et Michel A., « Coronavirus : les escrocs tentent de profiter de la crise », Le monde, 21 mars 2020 ; DGCCRF, « Arnaques liées au coronavirus », 27 mars 2020.

[40] Laville P., « Coronavirus : une société pharmaceutique escroquée de 6,6 millions d'euros », Le Parisien, 19 mars 2020.

[41] Piel S. et Michel A., « Coronavirus : les escrocs tentent de profiter de la crise », Le monde, 21 mars 2020 ; DGCCRF, « Arnaques liées au coronavirus », 27 mars 2020.

[42] Thibert C., « Ces fausses infos qui circulent sur le coronavirus », Le figaro, 30 janv. 2020.

[43] Commission européenne, Communiqué de presse, « Lutter contre la désinformation en ligne : un groupe d'experts préconise davantage de transparence de la part des plateformes en ligne », 12 mars 2018 ; Ce comportement est incriminé en France par loi du 29 juillet 1881 sur la liberté de la presse.

[44] V. à titre d'illustration : Article du Gouvernement, « CORONAVIRUS – COVID-19 : Appel au renforcement des mesures de vigilance cybersécurité », 19 mars 2020 ; Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes – Rapport sur la cybercriminalité*, fevr. 2014, p. 103.

[45] V. à titre d'illustration, Europol, « How criminals profit from the Covid-19 Pandemic », Press Release, 27 mars 2020 ; Parlement européen, « Comment vous protéger contre la cybercriminalité », Actualité, 1er avr. 2020.

[46] V. à titre d'illustration : Interpol, « Interpol met en garde contre les escroqueries financières liées à la Covid-19 », 13 mars 2020.

[47] Kigerl A., « Mettre fin au processus de l'émergence de la cybercriminalité : des délinquants motivés aux cyberattaques », *in Rapport du centre international pour la prévention de la criminalité, Prévention de la criminalité et sécurité quotidienne : prévenir la cybercriminalité*, 6e éd., 2018, p. 77.

[48] Rapport du ministère de l'Intérieur, *État de la menace liée au numérique en 2019*, mai 2019, rapp. n° 3, p. 32 ; Nocetti J., « Introduction », *in* « Cybersécurité : extension du domaine de la lutte », Politique étrangère 2018,

l'infraction, sa réalisation apparaît neutralisée, mais dans un contexte de crise sanitaire mondiale, les esprits critiques ne se seraient-ils pas égarés dans l'omniprésence voire l'omnipotence des réseaux ?

p. 13 ; Boos R., *La lutte contre la cybercriminalité au regard de l'action des États*, *thèse*, 2016, université de Lorraine.