LA PLACE DU DROIT PÉNAL DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ

GUILLAUME BEAUSSONIE

Référence de publication : Beaussonie, Guillaume (2021) *La place du droit pénal dans la lutte contre la cybercriminalité.* La Semaine Juridique édition générale (n°21). p. 964-967.

LA PLACE DU DROIT PÉNAL DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Le Club des juristes a rendu public en avril 2021 un rapport intitulé « Le droit pénal à l'épreuve des cyberattaques »Il existe en effet un droit pénal adapté à la lutte contre la cybercriminalitéPour être effectif, ce droit doit continuer à être adapté et être combiné avec d'autres outils juridiques

Il est difficile de nier que nous vivons dans une société « numérique », peu n'étant pas dotés de ces machines algorithmiques que l'on appelle des « ordinateurs », à laquelle tous ou presque associent une connexion au réseau informatique mondial qu'est Internet. Par utilité ou par nécessité, un nombre incalculable d'informations - de « données », si l'on préfère - sont ainsi générées, mobilisées et échangées, mais aussi, par là-même, exposées. Or, la patience et la prudence qui seraient de mise dans leur maniement ne sont pas toujours promues dans un contexte où, pour des raisons que nul n'ignore hélas, on encourage plutôt au « télétravail ». Il semble donc indispensable de sécuriser cet « univers de communication et de partage composé d'infrastructures, de réseaux et de systèmes d'information (SI), ainsi que de communications électroniques, qui sont interconnectés au monde entier, même spatial », qu'est le « cyberespace » (*V. Club des juristes, Le droit pénal à l'épreuve des cyberattaques, rapp., avr. 2021, p. 11 : https://www.leclubdesjuristes.com/wpcontent/uploads/2021/04/rapport_cyberattaques_DEFweb-1.pdf . - V. QR Code*) .

La « cybercriminalité », en effet, « définie, par le groupe de travail interministériel présidé par le procureur général Marc Robert, comme les faits constituant des infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication et des données qu'il recèle » (*Rapp., p. 12*), apparaît en plein essor ces dernières années. Encore récemment, au cours du mois de mai 2021, une « cyberattaque » n'a fait rien de moins que de provoquer la fermeture du plus grand oléoduc d'essence américain. On sait, aussi, la menace grandissante que représente « le croisement des cyberattaques et du terrorisme » (*A. Lepage, rapp., préface, p. 4*).

Pour ces raisons, en France comme à l'étranger, les travaux se multiplient, qui encouragent opportunément au renforcement de la lutte contre cette « cyberdélinquance ». Le Club des juristes a, en ce sens, rédigé deux rapports correspondant à deux volets complémentaires de la présente lutte : d'un point de vue en quelque sorte préventif, un premier rapport a été publié en janvier 2018 portant sur l'assurance du « risque Cyber » ; d'un point de vue répressif, vient d'être dévoilé, en avril 2021, un second rapport consacré, cette fois, au « droit pénal à l'épreuve des cyberattaques ». C'est au contenu de ce dernier que nous nous intéresserons.

La construction de ce rapport est assez classique : deux parties analysent le droit pénal positif en matière de cybercriminalité, l'une, intitulée « Traitement juridique des cyberattaques et conséquences économiques et sociales », étudiant les infractions applicables, l'autre, nommée « Cyberattaque : quelle réponse judiciaire ? », présentant les procédures qui peuvent être mises en œuvre. Une dernière partie, plus courte, synthétise les propositions, 10 en l'occurrence « pour faire avancer la lutte contre la cybercriminalité », le professeur Agathe Lepage y ajoutant une onzième, à savoir « ne […] pas oublier le bon sens élémentaire : prudence reste mère de sûreté, même dans le numérique, surtout dans le numérique » (*Rapp., préface, p. 5*).

C'est, finalement, de la place du droit pénal dans la lutte contre la cybercriminalité dont il est question dans ce rapport du Club des juristes. Il ressort de ce travail, en substance et dans l'air du temps, que même si un effort a déjà été fait pour ajuster l'ensemble des éléments du système répressif à cette forme originale et croissante de criminalité, ce système ne saurait lui-même représenter qu'un élément - évolutif - au sein d'un ensemble juridique plus large. Autrement dit, s'il faut adapter le droit pénal (**1**) pour bien lutter contre la cybercriminalité, il faut également, dans ce même but, le combiner avec d'autres droits (**2**).

1. ADAPTER LE DROIT PÉNAL

Ce premier aspect du travail du Club des juristes était assez attendu : il est évident, en effet, que le droit pénal doit être adapté à la particularité de la cybercriminalité. Ainsi, classiquement, face à l'essor d'une délinquance spécifique (**A**), s'est petit à petit construit un droit spécial (**B**).

A. – La spécificité de la cybercriminalité

C'est l'introduction du rapport qui, en bonne méthode, insiste sur ce point. L'« ambivalence du numérique », en effet, est d'être « porteur de croissance et d'innovation » tout en étant « proie à l'exploitation malveillante de ses failles et vulnérabilités » (*Rapp., p. 8*). Au-delà de comportements notoires que tout le monde garde en tête (ex. récent : les cyberattaques dont a fait l'objet le CNED), les chiffres révèlent que, en réalité, nul n'est prémuni contre de tels faits. Pratiquement toutes les entreprises - victimes principales de la cybercriminalité selon le rapport - y sont confrontées et les coûts directs et indirects des attaques numériques s'avèrent, pour elles, extrêmement élevés. Le contexte de la pandémie, avec ce qu'il implique de recours accru au télétravail, a au surplus conduit à la multiplication de ces attaques. Pour autant, comme le relève pertinemment M. Guillaume Poupard, le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), « quand la crise sanitaire s'arrêtera, la crise cyber perdurera » (*Rapp., p. 9*), à plus forte raison parce que des projets actuels, à l'instar du « Campus cyber », impliqueront également une forte mobilisation du numérique.

La difficulté de la lutte réside dans les caractères de cette délinquance : rentable, immatérielle et protéiforme.

Tout d'abord, c'est une délinquance dont le rapport risque/coût/gain est très favorable, des kits peu onéreux étant aisément accessibles sur le *darknet*.

Ensuite, c'est une délinquance lointaine, l'infraction étant la plupart du temps commise à un endroit de la planète alors qu'elle est ressentie à un autre.

Enfin, c'est une délinquance dont les formes sont variées, malgré un principe qui demeure le même. Le recours à l'ordinateur et au réseau n'empêchent effectivement pas une grande diversité des modes opératoires, que le rapport détaille et définit : *ransomwares* (rançongiciels), attaques en déni de service ou DDoS, *cryptojacking*, fraude au faux support informatique, *phishing* (hameçonnage), espionnage économique, sabotage et hacking de logiciel (*Rapp., p. 13 s.*).

B. – La spécialisation du droit pénal

Spécial par essence, le droit pénal l'est de plus en plus depuis que l'on a commencé à créer, en sus des incriminations, des procédures propres à certaines formes de délinquance. La cybercriminalité n'échappe pas à la règle.

Le rapport fait très justement remonter ce phénomène à la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, plusieurs autres ayant suivi, essentiellement la loi Godfrain n° 88-19 du 5 janvier 1988 relative à la fraude informatique *(V. JCP G 1988, 3333, Étude H. Croze)* et, dernièrement, la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la Justice (LPJ) qui a notamment prévu l'extension du recours à l'enquête sous pseudonyme et l'harmonisation des techniques spéciales d'enquête en matière de lutte contre la cybercriminalité (*Rapp., p. 13*).

Il en ressort, du point de vue des infractions, objet de la première partie du rapport (*Rapp., p. 19 s.*), soit une spécificité du mode opératoire incriminé, soit une spécificité du mode opératoire emprunté. Autrement dit, cohabitent des infractions spécifiques et des infractions classiques, toutes contribuant, à leur façon, à appréhender la cybercriminalité.

Concernant les premières, sont essentiellement concernées les atteintes aux systèmes de traitement automatisé de données (STAD : « ensemble composé d'unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, devant être protégé par des dispositifs de sécurité » selon le Rapport (*p. 20*)) incriminées aux articles 323-1 et suivants du Code pénal depuis la loi Godfrain, qualifiée de « visionnaire » par le rapport (*Rapp., p. 20 s.*).

Il est vrai que ce droit , délaissé pendant plusieurs années, a plus de vivacité ces derniers temps, à l'aune des réformes dont il a fait l'objet pour lui permettre de protéger davantage les données contenues par le STAD que le STAD lui-même, ce qui n'était pas prévu initialement. C'est bien sur cet aspect « informationnel » que le rapport insiste, soulignant la défense particulière instaurée pour les données personnelles par les articles 226-16 et suivants du Code pénal (*Rapp., p. 30*). Il s'agit alors de préserver des données auxquelles les entreprises ont accès, mais dont elles ne sont pas propriétaires, de sorte que leur propre responsabilité peut être engagée si on leur dérobe, c'est-à-dire en cas de « défaut de sécurisation » (*Rapp., p. 29*). Quant aux données patrimoniales, c'est tant pour sanctionner directement leur appropriation frauduleuse que, plus indirectement, en raison des conséquences sur le fonctionnement et sur l'image de l'entreprise de tels comportements,

que ceux-ci sont prohibés (*Rapp., p. 27*). Ces différentes protections apparaissent d'autant plus nécessaires que l'ensemble de ces données sont de plus en plus exposées à mesure que se développent les objets connectés (*Rapp., p. 21*).

Concernant les infractions classiques, il ne s'agit que de constater que le cyberespace peut en constituer le domaine : escroquerie, bien sûr, mais aussi usurpation d'identité, qualifications sur lesquelles le rapport revient principalement. Toutefois, comme le texte le précise, « toute infraction commise par internet ou au moyen des technologies de l'information et de la communication a vocation à entrer dans le champ de la cybercriminalité au sens large » (*Rapp., p. 42*). Aussi pourrait-on y faire figurer, par exemple, les harcèlements moral et sexuel, le législateur ayant dernièrement envisagé cette hypothèse (*C. pén., art. 222-33, I, al. 2, art. 222-33-2-2, al. 2*). En revanche, le silence du rapport sur le vol d'informations est éloquent : sans doute faut-il comprendre que, avec la majorité de la doctrine, ses auteurs entendent que ce comportement soit sanctionné, non sur le fondement de l'article 311-1 du Code pénal , comme c'est le cas actuellement, mais sur celui de l'article 323-3.

Du point de vue de la procédure, objet de la deuxième partie du rapport (*Rapp., p. 47 s.*), la spécialisation intéresse les acteurs aussi bien que le déroulement du procès.

Concernant les acteurs, plusieurs services d'enquête spécialisés ont été créés ces dernières années, comme l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), pour la Police nationale, le Centre de lutte contre les criminalités numériques (C3N), pour la Gendarmerie nationale, ou la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) pour la Préfecture de police de Paris. Par ailleurs, au sein des innombrables procédures particulières du Livre IV du Code de procédure pénale, figure un Titre XXIV consacré aux atteintes aux STAD et autorisant, notamment, que le procureur de la République de Paris, le pôle de l'instruction, le tribunal judiciaire et à la cour d'assises de Paris disposent d'« une compétence concurrente nationale » pour ces atteintes aux STAD ainsi que pour les « atteintes aux intérêts fondamentaux de la nation (cybersabotage), pour les affaires complexes et étendues géographiquement » (*Rapp., p. 54*). Et, au sein de la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO), toujours à Paris, la division J3 du parquet parisien est chargée de la lutte contre la cybercriminalité.

Ces différents acteurs collaborent bien sûr les uns avec les autres, mais aussi avec l'ANSSI, autorité nationale de la sécurité des systèmes d'information et différentes autorités administratives

indépendantes, telles l'Autorité des marchés financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR), ou encore avec TRACFIN, qui dispose d'une cellule « cybercriminalité ». À l'international, la cybercriminalité étant « par essence mondiale et sans frontières » (*Rapp., p. 59*), Europol, l'agence européenne spécialisée dans la répression de la criminalité, et Interpol, qui ont signé un accord de coopération en 2001, sont mobilisées en la matière. Plus spécifiquement, un Centre européen de la lutte contre la cybercriminalité (EC3) a été créé en 2013 « pour faciliter une coopération opérationnelle et analytique européenne entre les services répressifs, le milieu universitaire et le secteur privé » (*id.*), et un Complexe mondial Interpol pour l'innovation (CMII), spécialisé dans la lutte contre la cybercriminalité, l'a été en 2015, à Singapour, afin d'œuvrer « pour l'amélioration des compétences techniques des services d'enquête et le développement des outils transnationaux » (*Rapp., p. 60*). D'autres évolutions sont en cours, notamment dans le but de faciliter l'accès transfrontalier aux preuves électroniques.

Concernant la procédure, le rapport rappelle assez précisément les règles applicables pour les plaintes et la nécessité de faire preuve de célérité (*Rapp., p. 63 s. ; préconisation n° 10*). Il est possible, depuis l'entrée en vigueur sur ce point de la LPJ, de déposer une plainte simple en ligne. C'est alors que, si cela s'avère opportun, sont susceptibles d'opérer la spécialisation et la coordination qui viennent d'être présentées. L'enjeu, comme toujours en procédure pénale, sera de recueillir une preuve qualifiée par le rapport de « numérique » (*Rapp., p. 70 s.*). Les informations ainsi appréhendées sont, à la fois, difficiles à obtenir et à conserver. D'une part, elles peuvent provenir de très loin et, le cas échéant, être chiffrées. D'où différents moyens propres donnés aux enquêteurs pour agir efficacement : réquisitions d'entreprises qui détiennent des documents liés à l'enquête de leur remettre des données ; perquisitions et saisies informatiques ; enquêtes sous pseudonyme (*à simplifier encore, selon le rapport : préconisation n° 5*) ; accès aux correspondances stockées ; réquisitions de détenteurs des codes verrouillant l'accès à un contenu informatique de leur remettre les informations permettant d'y accéder (*un refus étant réprimé, par C. pén., art. 434-15-2 de 3 ans d'emprisonnement et 270 000 € d'amende*) ; recours à des experts judiciaires. D'autre part, les règles de conservation des données numériques par les opérateurs de télécommunication ne sont pas les mêmes d'un État à un autre, ce qui est une source de difficulté. Fixée à un an en France (*CPCE, art. L. 34-1, III*), elle n'est pas une obligation générale aux États-Unis et, dans le cadre de l'Union européenne, sa portée est incertaine à la suite d'un arrêt un peu étrange rendu par la Cour de justice le 8 avril 2014 (*aff. C293/12 et C594/12, Digital Rights Ireland*

: JurisData n° 2014-008774). Aussi le rapport préconise-t-il l'« adoption d'un régime européen de conservation des données permettant de répondre aux besoins opérationnels des services répressifs et judiciaires » (*préconisation n° 6*).

Plus globalement, le rapport encourage surtout à affermir cette spécialisation, notamment en créant une filière de « cybermagistrats » (*préconisation n° 2*) et en étoffant les différents services compétents (*préconisation n° 4*). Mais, même à ce point spécialisé, le droit pénal ne saurait suffire à combattre la cybercriminalité.

2. COMBINER LE DROIT PÉNAL

Sans doute moins attendu que le premier, bien qu'étant devenu assez habituel aujourd'hui, un second aspect du rapport du Club des juristes révèle la nécessité, pour le droit pénal , de cohabiter avec d'autres dispositifs de lutte contre la cybercriminalité, que ce soit au stade de la prévention (**A**) comme à celui de la répression (**B**).

A. – La prévention

Au-delà du premier rapport du Club des juristes consacré à l'assurance du « risque Cyber », et dont le présent rapport dresse par ailleurs un bilan positif (*Rapp., p. 77*), il est préconisé aux entreprises d'« investir dans la prévention contre les cyberattaques » (*préconisation n° 9 ; v. aussi p. 36*). Il s'agit de les encourager, dans le cadre du dispositif de gestion globale des risques, à faire des investissements « humains (par exemple, formation à la cybersécurité), techniques (investissement dans des logiciels, outils de sauvegarde, audits, etc.), organisationnels (mise en place d'une cybergouvernance) et assurantiels ».

C'est dire que, loin de se contenter des aspects dissuasif et punitif du droit pénal , la lutte contre la cybercriminalité doit certainement intégrer d'autres actions, telles que la « cybersécurité » et la « cyberdéfense ». La première est « l'état recherché pour permettre à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles », où la seconde représente « un ensemble de

mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels » (*Rapp., p. 12*). Dans un cas comme dans l'autre, on le constate, le droit pénal ne constitue qu'un élément constitutif ou complémentaire d'un ensemble qui ne saurait se contenter de ses solutions trop radicales, trop incertaines et trop tardives.

L'idéal, ainsi, serait de contrer la cybercriminalité en amont en la rendant, à la fois, plus difficile et moins rentable. Il appartient alors à tous, particuliers, entreprises et opérateurs de télécommunication essentiellement, de renforcer les dispositifs de lutte , le risque étant néanmoins que les délinquants s'adaptent progressivement à ces changements. En cela ne peut-on malgré tout pas se passer d'un droit pénal en la matière, à la condition bien sûr qu'il soit véritablement effectif, substantiellement et procéduralement, d'où l'existence et les propositions du présent rapport (*V. ci-dessus*).

B. – La répression

Au stade ultime de la répression, bien qu'étant alors dans leur domaine naturel, le droit pénal et ses acteurs sont également épaulés, voire supplantés par d'autres règles et d'autres acteurs, selon un processus désormais usuel en France.

Ainsi, en ce qui concerne les données personnelles, c'est moins le juge pénal que la Commission nationale de l'informatique et des libertés (CNIL) qui joue le rôle le plus important, à plus forte raison depuis l'adoption du règlement européen sur la protection des données (RGPD). Comme le rappelle le rapport, « les violations des dispositions concernant la sécurité des données peuvent être sanctionnées par une amende administrative d'un maximum de 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu » (*Rapp., p. 29*), ce qui a déjà pu conduire au prononcé de fortes sanctions pécuniaires à l'encontre de quelques entreprises notoires (*ex. : 400 000 € d'amende contre la société Uber en décembre 2018*).

Le droit pénal des données personnelles est, quant à lui, assez peu connu et mis en œuvre, mais il n'en doit pas moins être coordonné avec ces autres règles, qu'il s'agisse d'apprécier les responsabilités d'une entreprise et de ses membres en considération de l'organisation qui leur est imposée par le RGPD en vertu du principe d'« *accountability* » ou d'envisager que l'on cumule des

sanctions pénales et des sanctions administratives pour des faits qui, « en substance » (*CEDH, 10 févr. 2009, n° 14939/03, Zolotoukhine c/ Russie*), sont pourtant les mêmes. Le rapport, à cet égard, sans doute parce que la question ne s'est pas vraiment posée, est assez succinct (*p. 33*), la possibilité d'un tel cumul n'étant pas si certaine, même si, en effet, il existe un consensus sur la limitation de ses conséquences par application du principe de proportionnalité.

En ce qui concerne les données patrimoniales, la répression pénale n'est pas tant concurrencée qu'elle n'est renforcée par l'intervention de l'ANSSI, dont l'un des objets est de favoriser la circulation des informations techniques entre les différents services compétents, en ce compris les services judiciaires (*Rapp., p. 10 et 59*). Ce recours à un expert unique, extérieur et désintéressé apparaît salutaire, la spécialisation de la magistrature - par ailleurs prônée, comme nous l'avons souligné (*V. ci-dessus*) - semblant, malgré les vœux du rapport, difficile à réaliser en l'état des moyens consacrés à la Justice.

À la fin du rapport, M. Bernard Spitz, qui a présidé la commission l'ayant établi, rappelle les grands enjeux de la lutte contre la cybercriminalité : pour tous, les libertés, qu'il s'agit autant de préserver que d'encadrer ; pour les entreprises, la compétitivité, qu'il faut garantir ; pour l'État, la souveraineté, certainement en danger face à un péril croissant mais évanescent. Le droit pénal , à condition qu'il soit adapté et complété, demeure sans aucun doute l'un des boucliers à dresser contre ces assauts du XXI^{e} siècle.