Lutter contre la cybercriminalité : une priorité stratégique pour 2022.

Myriam QUEMENER
Avocat général
Docteur en droit

La disruption numérique[1] qui concerne désormais aussi bien les particuliers, les entreprises que les collectivités territoriales, apporte des améliorations indéniables aussi bien dans le quotidien que dans la gestion des organisations. Ce changement présente à la fois des avantages, tels qu'une plus grande agilité pour s'adapter aux nouveaux modes de fonctionnement et une réduction des coûts, mais également des inconvénients, comme la perte de visibilité de leurs actifs Internet, les incidents de sécurité, les violations, les atteintes à l'e-réputation.

Le constat

Selon une étude récente de l'éditeur de logiciels de cybersécurité McAfee [2]et du Centre d'études stratégiques et internationales (CSIS), la cybercriminalité, avec ses réseaux de plus en plus organisés, laisse derrière elle une note de plus de 1.000 milliards de dollars. Ce chiffre démontre l'ampleur des préjudices subis qui nécessitent des réponses pertinentes pour lutter contre ce fléau qui suppose, non seulement de la prévention, mais aussi la répression[3].

La gravité et la fréquence des cyberattaques contre les entreprises continuent d'augmenter à mesure que les techniques évoluent et que le travail à distance se développe. Avec l'essor du télétravail et le virage du numérique, jamais il n'a été aussi important de se protéger sur Internet, de choisir un antivirus pour son ordinateur, ou encore de faire attention aux newsletters et formulaires de commandes où l'on doit rentrer nos coordonnées.

Il est indispensable d'anticiper les crises liées aux cyberattaques, notamment dans le cadre d'une stratégie globale de cybersécurité : cloisonnement des systèmes, socle de sécurité opérationnel (SOC) avec en particulier la sensibilisation et un plan de

[1] « Le droit face à la disruption numérique », Myriam Quéméner, Lextenso, 2018

[2] https://business.lesechos.fr/entrepreneurs/numerique-cybersecurite/0610096243873-cybercriminalite-la-facture-ne-cesse-de-s-alourdir-341090.php

[3] « Quels droits face aux innovations numériques ? », Myriam Quéméner, Clément Wierre, Frédérique Dalle, Lextenso, 2020

continuité d'activité (PCA), au-delà d'un simple plan d'urgence, afin de préserver l'ensemble du patrimoine informationnel nécessaire.

Au niveau de la cyberdéfense, on constate un effort budgétaire important, ce qui est des plus justifiés. Ainsi, pour 2022[4], les crédits destinés à la coordination de la sécurité et de la défense, qui comprennent les moyens du Secrétariat général de la défense et de la sécurité nationale (SGDSN), les fonds spéciaux et les crédits du groupement interministériel de contrôle (GIC), sont confortés (+21,13 M€ en crédits de paiement).
Il conviendrait, dans le contexte actuel, d'augmenter également le budget de la justice pour traiter plus efficacement le volet contentieux de la cybercriminalité.

Les pistes d'amélioration

Ce contentieux en pleine expansion regroupe toutes les infractions pénales, tentées ou commises, à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet[5]. La cybercriminalité se manifeste ainsi notamment à travers les fraudes numériques qui se réalisent souvent par le biais de piratages, de cyberattaques et de manipulations informatiques. Elles ont pour objectif principal la récupération de données sensibles ou personnelles, qui sont par la suite facilement monnayables.

A l'heure d'un contexte économique difficile où l'on assiste à une pandémie non seulement sanitaire mais numérique, il est ainsi urgent de réaffirmer une stratégie et une politique pénales fortes en matière de lutte contre la cybercriminalité.

L'amélioration de la lutte contre la cybercriminalité passe par un renforcement de la coopération policière et judiciaire, tant sur le plan européen que sur le plan international. Il est urgent de créer une filière de cybermagistrats, au besoin par le biais d'une formation diplômante (DU Cyber par exemple).

Il faut inévitablement renforcer le pôle Cyber au niveau du parquet de Paris ainsi que la spécialisation d'une chambre du tribunal judiciaire en matière de droit du numérique et cybercriminalité. Il conviendrait également, au niveau de la cour d'appel de Paris, de mettre en place un département dédié au numérique et à la cybercriminalité, composé de magistrats du siège et du parquet. Il faut aussi accentuer les formations communes ENM/EFB et PN/ GN/Douanes sur le droit du numérique et la lutte contre ce fléau, avec davantage de stages pratiques dans les services spécialisés. Il est enfin indispensable que ce cybercontentieux soit clairement identifié dans les structures judiciaires.

A la veille de la présidence française de l'Union européenne à compter de janvier 2022, il est fondamental de préparer des arguments afin que ce fléau soit pris en compte prioritairement[6], assorti de moyens plus adaptés à son ampleur.

[4] Rapport d'information n° 219, au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat sur la coordination du travail gouvernemental (cyberdéfense, SGDSN), par Olivier Cadic et Mickaël Vallet
[5] « Protéger les internautes, rapport sur la cybercriminalité », groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014 https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000372.pdf
[6] « Le droit pénal à l'épreuve des cyberattaques », rapport du club des Juristes, avril 2021 https://www.leclubdesjuristes.com/les-commissions/publication-du-rapport-le-droit-penal-a-lepreuve-des-cyberattaques/