Institution judiciaire et lutte contre la cybercriminalité : orientations et perspectives

Myriam QUEMENER
Avocat général près la Cour d'appel de Paris
Docteur en droit

La cybercriminalité est devenue un véritable fléau et a coûté plus de 6000 milliards de dollars (5.700 milliards d'euros[1]) au monde l'an dernier selon le patron du géant italien de l'aéronautique et de la défense Leonardo, Alessandro Profumo. Le nombre d'attaques informatiques signalées à l'ANSSI [2] (Agence nationale de la sécurité des systèmes d'information) a augmenté de 37% entre 2020 et 2021.

Par ailleurs, la cybercriminalité est de plus en plus une délinquance financière et organisée. Cet aspect est d'ailleurs souligné par le dernier rapport du GAFI[3] : la transformation technologique du secteur financier, notamment avec l'apparition de nouveaux produits comme les actifs numériques, crée de nouvelles vulnérabilités. La nature transfrontalière de ces nouveaux services et la digitalisation complète des relations d'affaires continuent aussi de poser des défis en constante évolution, en particulier dans un contexte où le recours à ces nouveaux dispositifs se matérialise de manière croissante dans les affaires de blanchiment et de financement du terrorisme.

Outre la lutte contre les cyberattaques qui portent atteinte aux intérêts fondamentaux de l'État, le rapport relève que l'on assiste au développement d'une cybercriminalité de masse. La traditionnelle économie souterraine se trouve complétée par une cyber économie parallèle qui constitue une menace criminelle certaine, mais également un trouble à l'ordre public et judiciaire tant le nombre de particuliers victimes est en augmentation, comme l'ont démontré les attaques dont certains hôpitaux ont été victimes en février 202.

Dans ce contexte, il convient de présenter les dernières orientations de l'institution judiciaire en matière de lutte contre la cybercriminalité ainsi que les perspectives à envisager.

Une politique pénale pour la lutte contre la cybercriminalité

Le nouveau rapport de politique pénale du garde des Sceaux [4] déposé au Parlement en mai 2022[5]

[1]https://www.lefigaro.fr/secteur/high-tech/la-cybercriminalite-a-coute-plus-de-6000-milliards-de-dollars-en-2021-20220510
[2]https://www.ssi.gouv.fr/uploads/anssi_rapport_activite_2021_fr.pdf
[3]https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Rapport-Evaluation-Mutuelle-France-2022.pdf

[4]http://www.justice.gouv.fr/publications-10047/rapports-thematiques-10049/rapport-de-politique-penale-du-garde-des-sceaux-2021-34404.html
[5]Rapport établi conformément à l'article 30 du code de

aborde la lutte contre cybercriminalité dans la partie du document concernant l'accompagnement des évolutions de la société. Compte tenu de l'ampleur de ce fléau, il gagnerait même à l'avenir à figurer dans la partie du rapport sur le renforcement des politiques pénales prioritaires.

Il faut également noter que la direction des affaires criminelles et des grâces (DACG) avait déjà en 2021[6] fixé les axes stratégiques afin que soient regroupées à la juridiction parisienne les cyberattaques par rançongiciel.

L'ANSSI et le ministère de la justice ont aussi publié un guide pour sensibiliser les entreprises et les collectivités[7].

Le ministère de la Justice a mis en place une politique pénale dynamique afin de répondre aux évolutions des phénomènes cybercriminels, en s'engageant notamment, avec les partenaires interministériels, auprès du Secrétariat général de la défense et de la sécurité nationale (SGDSN) pour contribuer aux travaux stratégiques en matière d'atteintes cyber aux intérêts fondamentaux de l'État et pour consolider chacun des acteurs dans la poursuite de ses finalités, en particulier, pour ce qui concerne l'autorité judiciaire, l'action de la section J3 du parquet de Paris composée de magistrats spécialisés en la matière.

En plus du développement des plateformes de signalement en ligne de ces infractions gérées par le ministère de l'Intérieur, les services du ministère de la Justice accompagnent la création d'un observatoire de la menace cyber afin de mieux connaître l'ampleur de cette cybercriminalité. Concernant la cybercriminalité de haute intensité, le parquet de Paris, au titre de sa compétence concurrente, a connu une augmentation qui donne lieu à des développements inquiétants et nécessite à la fois des actions de sensibilisation et des travaux à l'international.

Enfin, il faut souligner que des magistrats «cyber-référents» formés et identifiés au sein de chaque parquet sont régulièrement réunis par la chancellerie (DACG) et fonctionnent en réseau, ce qui permet de renforcer le niveau de spécialisation et de prise en compte judiciaire de ce contentieux en évolution permanente.

La lutte contre la haine en ligne

Le rapport de politique pénale du garde des Sceaux présente le pôle national de lutte contre la haine en ligne [8](PNLH) créé en janvier 2021 au sein du tribunal judiciaire de Paris, chargé de centraliser, sous la direction du procureur de Paris, le traitement des affaires significatives de cyber-harcèlement et de haine en ligne[9]. Ce pôle a établi un véritable dialogue avec les opérateurs de réseaux sociaux. Doté de deux magistrats, trois greffiers, deux juristes-assistants et d'un assistant spécialisé, il doit permettre d'apporter une réponse visible et unifiée là où ce type de phénomène amenait souvent chaque parquet territorial à répondre aux seuls faits commis par les auteurs identifiés sur son ressort. Durant l'année 2021, le pôle a été saisi de 502 procédures, provenant en partie de la plateforme d'harmonisation, d'analyse,

procédure pénale

[6]Dépêche relative à la lutte contre la cybercriminalité de la Direction des affaires criminelles et des grâces DACG, ref / 2020 : 0064 /M12C

[7] Attaques par rançongiciels, tous concernés, https://www.ssi.gouv.fr/actualite/rancongiciels-face-a-lampleur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/

[8] https://www.lemonde.fr/societe/article/2021/07/08/les-debuts-discrets-du-pole-national-de-lutte-contre-la-haine-en-ligne_6087529_3224.html

[9]Circulaire relative à la lutte contre la haine en ligne, N° NOR : JUSD2032620C, 24 novembre 2020

de recoupement et d'orientation des signalements (PHAROS), rattachée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Outre la création de ce pôle et la participation de la direction des affaires criminelles et des grâces à l'observatoire de la haine en ligne, l'engagement du ministère de la Justice pour lutter contre cette haine en ligne s'est aussi traduit par l'adoption du décret n° 2020-1444 du 24 novembre 2020 pris pour l'application de l'article 15-3-3 du code de procédure pénale qui a désigné le tribunal judiciaire de Paris comme juridiction compétente disposant d'une compétence nationale concurrente pour les délits de harcèlement sexuel ou moral à caractère discriminatoire.

Les actions de coordination avec les associations, comme par exemple Respect zone[10], en matière de prévention sont également essentielles et doivent encore se développer.

De plus, la loi du 24 août 2021 confortant le respect des principes de la République a notamment créé un nouveau délit de mise en danger par la diffusion sur les réseaux sociaux de messages vindicatifs comportant des éléments permettant d'identifier ou de localiser une personne pour qu'il lui soit porté une atteinte grave (article 223-1-1 du code pénal), et a rendu applicable les poursuites accélérées pour les abus les plus graves de la liberté d'expression (comparution immédiate et convocation par procès-verbal). Enfin, les bonnes pratiques développées par les juridictions et les services déconcentrés sur cette thématique sont à relever.

L'accent sur les opérations internationales

La spécificité des cyber-enquêtes nécessite très fréquemment des investigations à l'étranger et donc de la coopération internationale, en particulier avec les États-Unis, afin d'accéder aux données de souscription de trafic ou de contenu nécessaires pour l'enquête.

Récemment, une opération de police internationale dénommée Tourniquet a permis d'arrêter les gérants du plus important site de revente de données piratées, RaidForums. Les investigations poussées des cyber-enquêteurs du Royaume-Uni, des États-Unis, d'Allemagne, de Suède, du Portugal et de Roumanie ont abouti au démantèlement total de cette plateforme criminelle.

RaidForums vendait en accès libre des bases de données volées appartenant à un certain nombre de sociétés américaines. L'infrastructure du réseau a été saisie et l'administrateur de la plateforme ainsi que deux de ses complices ont été arrêtés, affirme le site d'Europol.[11]

Le commerce du trafic de données sur RaidForums est apparu en 2015 et, très vite, ce site a accédé à une notoriété internationale en raison de la facilité avec laquelle ses utilisateurs récupéraient les informations subtilisées. N'importe qui, en fait, pouvait se les procurer contre une somme d'argent évidemment, et de préférence en monnaie virtuelle de type bitcoin.

L'institution judiciaire est très active au niveau des négociations à l'international. On peut citer par exemple le Protocole Additionnel à la Convention sur la cybercriminalité (« Convention de Budapest »), destiné à renforcer la coopération et la

[10] https://www.respectzone.org/

[11] https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

divulgation des preuves électroniques, qui a été ouvert à la signature lors d'une conférence internationale organisée les 12 et 13 mai à Strasbourg - sous la Présidence italienne du Comité des Ministres du Conseil de l'Europe. Le Protocole additionnel répond à ce défi et fournit des outils comme la coopération directe avec les fournisseurs de services et les bureaux d'enregistrement, des moyens efficaces d'obtenir des informations sur les abonnés et des données relatives au trafic, une coopération immédiate en cas d'urgence ou des enquêtes conjointes - qui sont soumis à un système de droits de l'homme et d'état de droit, y compris des garanties en matière de protection des données.

Perspectives

Il apparaît nécessaire que l'institution judiciaire continue dans cette voie en étoffant ses services spécialisés et ses compétences de façon encore plus lisible, non seulement en première instance mais également en appel. Il conviendrait aussi de désigner des magistrats du siège cyber-référents pour que la cybercriminalité soit systématiquement traitée comme un véritable contentieux à part entière. A cet égard, l'ouverture du Campus Cyber de la Défense[12], qui réunit entreprises, services de l'État, organismes de recherche et de formation dans un même lieu, crée un écosystème de cybersécurité où l'institution judiciaire a toute sa place et pourra échanger et mieux connaître ses interlocuteurs.

[12]https://campuscyber.fr/