Le traitement de la cybercriminalité par deux juges d'instruction spécialisés

Elise TREGUER
VP chargée de l'instruction
Pôle financier
Criminalité financière et cybercriminalité
JIRS - JUNALCO

Brice HANSEMANN
VP chargé de l'instruction
Pôle financier
Criminalité financière et cybercriminalité
JIRS - JUNALCO

Présentation du service CFC

Le tribunal judiciaire de Paris compte plusieurs pôles spécialisés de l'instruction dont le pôle financier composé de deux services : le service économique et financier (SEF) et le service de la criminalité financière et cybercriminalité (CFC). Anciennement dénommé service de la délinquance astucieuse, celui-ci a pris sa dénomination actuelle en septembre 2020 et vu ses effectifs de magistrats portés à 10. Cette période correspond également à l'année de mise en place, au sein du tribunal judiciaire de Paris, de la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO) dont le service CFC est une des composantes.

L'évolution récente du vocabulaire et l'ajout de la cybercriminalité dans la désignation du service en 2020 soulignent d'une part l'évolution de l'appréhension du phénomène de la délinquance économique et financière et d'autre part l'émergence d'un nouveau contentieux lié aux risques du numérique dans la sphère d'intervention de la justice, ces deux secteurs étant étroitement liés. En effet, le risque cyber, à savoir l'ensemble des risqués liés à l'usage des technologies numériques, et la criminalité financière se rejoignent à plusieurs titres et vont de pair avec la digitalisation de l'économie. La crise de la Covid 19 a accéléré cette tendance.

Si le juge d'instruction est souvent présenté comme un magistrat solitaire, les dossiers dévolus au service se prêtent souvent à la pratique de la cosaisine lorsque la gravité ou la complexité de l'affaire le justifie. Par ailleurs, le pôle financier dispose de plusieurs assistants spécialisés et attachés de justice qui apportent leur soutien aux magistrats instructeurs. Toutefois, avec un seul assistant spécialisé cyber actuellement, cette notion d'équipe autour du magistrat demeure peu étoffée alors que le service CFC fait pourtant face à des dossiers de plus en plus nourris sur un plan technique, ce qui n'est pas sans soulever quelques inquiétudes.

Ce service dispose de compétences particulières d'un point de vue géographique et matériel.

Il instruit les dossiers au titre :
- de la juridiction interrégionale spécialisée (JIRS) créée en 2004, pour les dossiers revêtant une grande complexité ;
- de la JUNALCO créée en 2019, opérant au tribunal judicaire de Paris exclusivement, en charge de la lutte contre la criminalité de très grande complexité ;
- de la compétence concurrente nationale (CCN) qui permet de centraliser des faits de nature cyber ayant lieu sur l'ensemble du territoire. Cette spécificité offre l'avantage de favoriser la cartographie des phénomènes criminels numériques, de permettre les rapprochements et de regrouper de manière cohérente les procédures afin d'élaborer une réponse pénale adaptée.

Panorama des types de dossiers traités

La cybercriminalité recouvre les crimes et délits commis à l'encontre ou par le biais des systèmes d'information. Le service CFC n'a donc pas vocation à traiter les affaires portant sur la haine et la diffamation en ligne, le cyberharcèlement et la pédopornographie en ligne notamment qui relèvent d'autres services de l'instruction.

L'essentiel des dossiers « cyber » traités par le service porte sur des infractions qui constituent le vecteur de la commission d'infractions relevant de la criminalité organisée et financière. Ainsi, le caractère hybride mentionné dans la dénomination du service trouve toute son expression. Au rang de ces dossiers, il est possible d'en établir une liste, non-exhaustive, qui occupe la majeure partie de nos cabinets :

- le déploiement de solutions de téléphonie chiffrée à des fins criminelles ;
- les atteintes aux systèmes de traitement automatisé de données (STAD) : rançongiciels ou faux supports informatiques ;
- les plateformes d'échanges de cryptoactifs (PSAN) qui contreviennent à la réglementation LBC-FT et participent à l'opacification des flux financiers illicites ;
- les escroqueries en bande organisée et fraudes de grande ampleur (notamment FOVI, fraude l'investissement du type pyramide de Ponzi ou pig butchering…)

Ont été traitées et sont toujours en cours des informations judiciaires portant sur le déploiement, par des organisations souvent implantées hors du territoire national (en Amérique du Nord notamment), de solutions de téléphonie chiffrée extrêmement sophistiquées par le recours à plusieurs couches de chiffrement et à une infrastructure technique robuste. A titre d'exemple, un dossier, récemment clôturé à l'instruction, a nécessité un investissement conséquent sur cinq années et s'est articulé par la mise en place de méthodes de travail et d'une synergie adaptées pour répondre aux multiples défis soulevés (en termes de ressources humaines, techniques et d'entraide internationale). La mise à jour de très nombreux phénomènes criminels de haute intensité a ainsi permis et permet encore, d'initier, voire d'alimenter, un nombre significatif de dossiers incidents conduisant au démantèlement d'infrastructures criminelles et à des interpellations sur l'ensemble du globe (atteinte à la vie, trafic international de stupéfiants, blanchiment de capitaux…). Les milliers d'interpellations, tant en France qu'à travers le monde, ont été sources d'un contentieux juridique au volume conséquent générant des jurisprudences très fournies, souvent novatrices, compte tenu des défis et problématiques posés par l'emploi de ces nouvelles technologies (portant notamment sur l'interception de masse ainsi que sur l'admissibilité des éléments de preuves recueillis au moyen d'interception et de captation judiciaires).

La quête d'anonymat se retrouve, par ailleurs, sur Internet par l'utilisation notamment de VPN qui, si elle n'est pas interdite, peut être utilisée pour masquer des activités illégales.

Si le nombre de cyberattaques ciblant les grandes enseignes ou entreprises est constant, on remarque que les groupes de rançongiciels ciblent de plus en plus les petites et moyennes entreprises en raison, sans doute, d'un moindre investissement de ces dernier dans la cyberdéfense. En effet, une simple analyse coûts-avantages oriente les cybercriminels vers les organisations disposant d'infrastructures moins sécurisées. La plupart des opérateurs de rançongiciels choisissent leurs cibles en fonction de la taille, de la probabilité d'un paiement et de l'effort requis pour compromettre les systèmes de la cible.

Le dark web, accessible principalement par le réseau Tor, constitue un catalyseur clé de la cybercriminalité, permettant aux délinquants de partager leurs connaissances, leurs outils et leurs services de manière plus dissimulée.

Les défis quotidiens auxquels nous sommes confrontés s'agissant du recueil de la preuve numérique dans le traitement des dossiers concernent principalement :

- l'indisponibilité des données, en particulier lorsqu'elles sont supprimées, en raison de règles incohérentes et inadaptées en matière de durée de conservation des données à des fins répressives ;
- l'impossibilité de récupération des données, en particulier en cas d'échec de l'extraction à partir d'un support numérique ;
- le caractère illisible / inintelligible des données, en raison du chiffrement ;
- l'impossibilité matérielle d'analyser les données dans toutes les situations ;
- la difficulté à obtenir les données, en raison de système juridiques différents.

La criminalité financière, principalement la fraude à l'investissement et le blanchiment d'argent, reste le domaine dans lequel les cryptomonnaies sont le plus souvent rencontrées. Plusieurs dossiers portent sur des plateformes de cryptoactifs, peu regardantes sur l'origine des fonds, parfois criminels, qui sont transférés par le biais de leur service. Cette opacification des fonds douteux est accentuée par l'absence de procédure de connaissance du client (KYC) ou le défaut de réponse aux autorités judiciaires ou policières lorsqu'elles sont légalement requises. Les principales difficultés auxquelles nous sommes confrontés dans ce type de dossier portent sur le traçage des flux de cryptos et l'identification des auteurs des transactions et détentrices des wallets.

Le phishing, sous toutes ses formes (le smishing : SMS/text phishing, le quishing : QR code phishing ou le vishing : hameçonnage vocal), constitue le vecteur le plus répandu d'attaque. La disponibilité du phishing-as-a-service ne cesse d'augmenter. Les kits d'hameçonnage sont largement disponibles, ce qui réduit le niveau d'organisation et d'expertise technique requis pour perpétrer des fraudes.

Services et techniques employés

Dans le cadre des informations judiciaires que nous traitons, nous sommes amenés à déléguer certains actes d'investigation (par commission rogatoire) dont nous conservons la direction des orientations judiciaires. Pour ce faire, dans le domaine de la cybercriminalité, nous avons principalement recours à des services d'enquête spécialisés relevant tant de la police nationale (OFAC), de la gendarmerie nationale (UN Cyber) ou de la Préfecture de Police (BL2C) ou encore DGSI. En appui, sur les compétences rares notamment (concernant les cryptoactifs), le COMCYBER-MI peut également être mobilisé. En raison de la thématique ou de la spécificité des dossiers, ces services ou offices peuvent être cosaisis avec d'autres offices centraux ou services territoriaux ou SR / BR…

De plus, le Ministère de l'Intérieur a mis en place trois plateformes de signalement d'infraction en ligne qui peuvent apporter des éléments de nature à enrichir les investigations en cybercriminalité : PERCEVAL (cartes bancaires), PHAROS (contenu illicite en ligne) et THESEE (escroqueries).

En réponse aux problématiques relevées dans les développements précédents et concernant notamment chiffrement, il peut être recouru à des techniques d'enquête numériques spéciales telles que l'interception, la captation, la géolocalisation, l'enquête sous pseudonyme, la perquisition numérique…). Afin d'exploiter les supports numériques, nous faisons également appel à des experts publics ou privés, notamment en cas de chiffrement des supports. Les recherches en sources ouvertes ou OSINT pour Open Source Intelligence constituent également un apport de plus en plus important pour les enquêtes.

Une entraide pénale intense

Le recours à la preuve numérique s'est développé avec la massification et la diversification de l'usage des appareils des outils de cette nature.

Le caractère transfrontalier de la criminalité organisée rend indispensable le développement d'outils permettant l'accès aux données contenues d'une part dans les supports numériques (téléphones, ordinateurs, clés cryptos… dont l'exploitation se fait généralement au cours d'une perquisition) et d'autre part dans les systèmes à distance (accès aux correspondances stockées qui

est opérées à l'insu de la personne concernée).

Ainsi, les magistrats instructeurs peuvent être amenés à se déplacer à l'étranger. Ils ont en effet les plus à même d'identifier les matériels nécessaires à la manifestation de la vérité dans le cadre de leur dossier. Leur présence, aux côtés des enquêteurs et/ou magistrats est décisive dans la mesure où ils sont en mesure d'identifier les supports numériques recherchés.

Le volet coopération, indispensable dans les dossiers « cyber », entre autorités judiciaires et policières, est amplement facilité enfin par la participation, à la demande des magistrats instructeurs, des agences européennes que sont Eurojust et Europol. A ce titre, Europol constitue un acteur incontournable compte tenu des moyens humains, logistiques et techniques à sa disposition : plateforme de déchiffrement, task force entre services d'enquête (OTF), plateforme d'Experts Europol (EPE), messagerie sécurisée…

Enjeux et perspectives : les défis sont nombreux, dont :

- l'Intelligence Artificielle dont les technologies dérivées élargissent les possibilités pour les fraudeurs d'atteindre plus de victimes à la fois et rendent l'ingénierie sociale encore plus efficace ;
- la 6G (prévue pour 2030) ;
- l'Internet des objets (IOC) ;
- la communications par satellites ;
- le développement de l'informatique quantique.