LIVRE BLANC

Les cyberinfractions

Identification des nouvelles menaces et élaboration de préconisations pour une réponse opérationnelle efficace à l'échelle européenne

Collège européen des investigations financières et de l'analyse financière criminelle

Remerciements

Ce rapport a été rédigé par un groupe de travail placé sous la direction de Madame Chantal CUTAJAR, directrice générale du CEIFAC et maître de conférences HDR de l'université de STRASBOURG. Il s'appuie sur les interventions et les contributions des différents intervenants à la conférence synthèse que le Collège a organisé en juin 2021, et en particulier sur les travaux de Madame Myriam QUEMENER, Madame Michelle ABRAHAM et Madame Denise GROSS.

Madame Chantal CUTAJAR, Monsieur Marc SIMON, Codirecteur du CEIFAC et l'ensemble des membres du collège souhaitent remercier tous les intervenants à cette conférence synthèse, colloque universitaire qui a mis en synergie d'éminents acteurs de la scène pénale européenne, réunis dans le but d'énoncer des propositions en vue d'améliorer les dispositifs européens et nationaux en vigueur.

Merci à :

- Michelle ABRAHAM, Avocat, France.
- Alain BAUER, Professeur de criminologie au Conservatoire National des Arts et Métiers, New York et Shanghai, PSD R3C - ESD R3C.
- Max BRAUN, Parquet général du Luxembourg, cellule de renseignement financier luxembourgeoise.
- Philippe DE KOSTER, Avocat général, Parquet de la Cour de cassation, Président de la CTIF.
- Denise GROSS, Docteur en droit, avocat, Argentine.
- Maryvonne LE BRIGNONEN, Directeur de TRACFIN.
- Myriam QUEMENER, Avocat général près la Cour d'appel de Paris, Docteur en droit, France.
- Marinne VACANDARE, Capitaine de Police, enquêtrice à la Division de Lutte contre la Criminalité Financière de la DTPJ de Lyon
- Adjudante Elena VALLEJO, SR STRASBOURG, Enquêteur Nouvelles Technologies, France.
- Benjamin VOGEL, Chercheur spécialisé, Institut Max Planck, Allemagne.

CONTACT

CEIFAC
Université de Strasbourg
Strasbourg Cedex (France) Tél.
+33 (0)3 68 85 65 92
Courriel : contact@ceifac.eu
Site internet : http://www.ceifac.eu

AVERTISSEMENT

Les points de vue exprimés dans ce rapport ne reflètent pas nécessairement les positions officielles des services représentés dans la formation ou des donateurs finançant ce projet. Les informations du présent document doivent s'interpréter au regard du droit et des procédures internes du pays et du service concernés, dans le respect de la protection des droits fondamentaux.

TABLE DES MATIERES

Remerciements 1
PROPOS INTRODUCTIFS 4
SYNTHESE DES RECOMMANDATIONS 6
1. COOPERATION POLICIERE ET JUDICIAIRE 6
2. CHARTE DES DROITS DES VICTIMES 7
TEXTES DE REFERENCE 8
LE CEIFAC – Présentation générale 9
L'ENQUÊTE : IDENTIFICATION DES MODUS OPERANDI 15
1. Un glossaire unifié et harmonisé relatif à la lutte contre les cyberinfractions 16
2. La traduction juridique des comportements criminels 19
3. Renforcer les capacités opérationnelles des enquêteurs européens 27
4. Envisager la création d'un parquet européen spécialisé en matière de cybercriminalité 29
5. Favoriser la création d'un réseau européen d'enquêteurs criminels spécialisés 32
6. La boîte à outils du cyber enquêteur 34
7. La charte des victimes de cyberattaque 54

PROPOS INTRODUCTIFS

Le livre blanc est la résultante du cycle de recherche consacré à la cybercriminalité, cycle composé de cinq colloques universitaires et d'une conférence synthèse, placé sous la direction de Mme Chantal CUTAJAR, directrice générale du CEIFAC et maître de conférences HDR de l'université de Strasbourg. Il vient clore un cycle dédié à la lutte contre le blanchiment d'argent et autres infractions réalisées grâce aux moyens et réseaux numériques et propose de concevoir des réponses pénales, tant législatives qu'opérationnelles en vue de lutter contre les phénomènes liés à la cybercriminalité.

En identifiant les comportements criminels, l'ingénierie mise en œuvre par les réseaux transnationaux dans le but de corrompre le système en vue de récolter des fonds à des fins criminelles, de faciliter les flux financiers ou encore de blanchir certains fonds illégaux, les moyens d'améliorer la coopération intra-européenne et extra-européenne (incidence en matière de recueil de la preuve, adoption de définitions communes, mise en place de procédures communes, …) et de concevoir un manuel de bonnes pratiques fondé sur une coopération efficace entre les services d'enquête et de justice au niveau européen, le CEIFAC s'est intéressé aux moyens de lutte ainsi qu'aux dispositifs qui permettraient d'établir une coopération efficace, dans le cadre d'une action proactive, des forces de l'ordre en mettant l'accent sur l'importance desdits comportements criminels, des réseaux utilisés et des moyens mis en œuvre (par exemple , en identifiant et en localisant les réseaux criminels en suivant le modèle des pratiques et procédures déjà en vigueur en matière de cyberpornographie).

Enfin, en posant un regard tout particulier sur l'importance de la prise en compte des victimes, en définissant la place, les droits et leurs rôles à chaque étape au cours de la procédure, les chercheurs du CEIFAC ont établi une liste de recommandations propices à l'amélioration des dispositifs nationaux et européens existants.

Dans cette entreprise, un certain nombre de points cruciaux ont été abordés au cours de différents colloques universitaires qui ont accueillis un grand nombres d'experts, lesquels ont produits des propositions rassemblées dans cet ouvrage et qui ont trait à l'identification des fraudes financières ; l'identification des escroqueries d'exploitation (publicité mensongère, trafic de faux médicaments, …) ; l'identification des offres d'opportunité d'investissements frauduleux (phishing), des collectes de fonds pour de fausses organisations caritatives ; l'étudie de l'ingénierie criminelle, l'identification des comportements récurrents, des *modus operandi*. Ils ont alors formulé des solutions pour lutter contre ces phénomènes et lutter contre la cybercriminalité, menace grave que ce soit pour les individus ou pour l'intégrité des systèmes informatiques mondiaux.

Dans une démarche fondée sur une analyse fine qui permette l'identification des comportements criminels , les chercheurs du CEIFAC ont identifié les obstacles aux investigations qu'ils soient d'ordre opérationnel ou réglementaire, proposent une méthodologie de travail harmonisée pour les autorités publiques européennes qui permette de rendre encore plus efficiente la lutte contre une délinquance organisée transfrontière qui use et abuse des nouvelles technologies, et *in fine*, initie une nouvelle approche de la matière fondée sur une méthodologie d'enquête et un accueil réinventé des victimes qui permette de prendre en compte leur statut de victime à juste titre.

SYNTHESE DES RECOMMANDATIONS

Ce Livre Blanc expose l'évolution de la situation, présente des solutions concrètes et formule deux ensembles de recommandations. Ces dernières, en bleu, figurent dans un encadré. Pour faciliter la lecture, elles sont également rassemblées ici de manière synthétique.

1. COOPERATION POLICIERE ET JUDICIAIRE

a. Renforcer l'impact de la Convention de Budapest.
b. Promouvoir son rayonnement dans les pays non-membres du Conseil de l'Europe et n'ayant pas encore ratifié le texte et les protocoles additionnels.
c. Donner une définition harmonisée de la cybercriminalité.
d. Proposer un glossaire des termes propres à la matière, glossaire disponible et fidèle dans toutes les langues européennes.
e. Pour l'année 2022, faire que la lutte contre la cybercriminalité soit proclamée grande cause nationale, européenne et internationale.
f. Identifier les points de contact nationaux, européens et internationaux.
g. Créer un parquet européen spécialisé dans la cybercriminalité sur le modèle du parquet financier pour lutter contre les cyberattaques visant les institutions de l'Union européenne.
h. Créer dans chaque État membre une chaîne pénale compète relais et interlocuteur privilégié de l'instance pénale européenne.
i. Améliorer les dispositifs de discussion et d'échange entre les acteurs de la chaîne pénale.
j. Développer et multiplier les offres de formations européennes telles que celles proposées par le CEIFAC qui mettent en synergie les représentants des forces de l'ordre et de la justice européenne.

2. CHARTE DES DROITS DES VICTIMES

a. Analyser les avantages et les inconvénients du dépôt de plainte.
b. Former des responsables de la prise en charge des victimes de cyberinfractions.
c. Adopter une charte européenne des droits des cybervictimes.
d. Contribuer à renforcer les prérogatives de celles et ceux qui ont subi une cyberattaque et réduire les risques d'une re-victimisation en :
favorisant l'accès à la justice, retravailler le recueil de la plainte et développer une écoute attentive et respectueuse,
facilitant l'accès aux informations liées à la procédure après le dépôt de la plainte,
développant l'interaction avec des professionnels formés à la matière, en assurant la transparence dans les démarches et les formalités relatives à la recevabilité de la plainte
procédant à une explication claire et différenciée entre le dépôt de plainte et le signalement,
révisant les délais pour déposer plainte,
précisant les conditions et les formalités pour demander réparation et le remboursement des frais de justice, les informations sur le droit à l'accompagnement pendant toutes les phases importantes de la procédure (y compris en cas d'investigation transfrontalière),
précisant le parcours de l'enquête, les voies de recours à chaque étape de la procédure,
renseignant sur les obligations des associations d'aides aux victimes (droits et limites à l'exercice d'une action),
donnant les obligations des fournisseurs de service Internet, celles des pouvoirs publics dans la protection des citoyens contre les infractions commises en ligne.
e. Accompagner la charte d'un guide et ses annexes qui soit adapté à chaque État membre et qui contienne les textes et réglementations applicables au niveau national, la liste des contacts utiles et un lexique des termes.
f. Créer un partenariat avec *Victim Support Europe* pour l'établissement d'une charte à visée globalisée et humaine.

TEXTES DE REFERENCE

Convention de Budapest, (STE n° 185), Budapest, 23.XI.2001

Projet de conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cyber malveillance ("boîte à outils cyber diplomatique"), n° 7923/2/17 REV 2, 7 juin 2017

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n°0062 du 15 mars 2011

Décisions-cadre 2002/584/JAI relative au mandat d'arrêt européen et aux procédures de remise entre les pays de l'UE, OJ L 190, 18.7.2002, p. 1–20

Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, OJ L 130, 1.5.2014, p. 1–36

Guide des droits de l'homme pour les utilisateurs, 16 avril 2014, *https://www.coe.int/fr/web/freedom-expression/guide-to-human-rights-for-internet-users*

Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques, COM/2021/718 final, *https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group*

Directive 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018 visant à lutter contre le blanchiment de capitaux au moyen du droit pénal, PE/30/2018/REV/1, *OJ L 284, 12.11.2018, p. 22–30*

Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil, JOUE L 123 du 10 mai 2019

Rapport d'information de Mme Sophie JOISSAINS et M. Jacques BIGOT, fait au nom de la commission des affaires européennes et de la commission des lois n° 613 (2019-2020), Cybercriminalité : un défi à relever aux niveaux national et européen, 9 juillet 2020

Genèse. Le Collège européen des investigations financières et de l'analyse financière criminelle, dénommé CEIFAC, est né de la mise en œuvre d'une préconisation faite à l'issue des Universités d'été des investigations financières et de l'analyse financière criminelle à l'échelle européenne organisées en juillet 2010 par le GRASCO (Groupe de Recherche-Action Sur la Criminalité Organisée), laboratoire de recherche de l'UMR DRES 7354.

Les « Universités d'été des investigations financières et de l'analyse financière criminelle » se sont tenues du 1er au 11 juillet 2010 avec le soutien financier des collectivités territoriales, la Ville et l'ancienne communauté urbaine devenue Eurométropole de Strasbourg et la Région Alsace. L'Université de Strasbourg a ainsi, avec la Gendarmerie nationale, l'Université de droit de Bari (Italie), La police judiciaire du Luxembourg et la *Guardia di finanza* italienne, répondu à un appel à projet de la Commission européenne sur un programme « Prévention et lutte contre la criminalité organisée » (ISEC 2009) pour organiser les « universités d'été des investigations financières et de l'Analyse financière criminelle » qui se sont tenues du 1er au 11 juillet 2010.

Plusieurs des recommandations formulées ont été prises en compte par la Commission pour construire la réflexion autour des investigations financières à l'échelle européenne, notamment par la communication COM (2008) 766 : Communication de la Commission au Parlement européen et au Conseil - Produits du crime organisé : garantir que « le crime ne paie pas » du 20 novembre 2008.

Une mission de formation et un outil de collaboration entre les services répressifs européens

Le diagnostic. En 2013, le rapport d'évaluation de la criminalité organisée grave (*Serious Organized Crime Threat Assessment* - SOCTA) d'EUROPOL révélait que plus de 3600 groupes criminels organisés (GCO), interconnectés, composés de membres de plusieurs nationalités étaient actifs dans l'UE et constituaient une menace sérieuse. Polycriminelles, ces organisations génèrent une véritable économie criminelle. Ses membres agissent sur le mode entrepreneurial. Le rapport mettait en évidence que les organisations criminelles sont impliquées dans un large éventail d'activités illicites et frauduleuses générant des profits substantiels. Les deux rapports suivants n'ont fait que souligner l'aggravation de ces constats.

Les obstacles à l'efficacité de la lutte contre les réseaux criminels au moyen des techniques d'investigation habituelles sont identifiés. Ils ont trait notamment à la capacité des organisations criminelles à utiliser des techniques financiers-juridiques très sophistiquées pour empêcher les enquêteurs d'identifier les têtes de réseaux et mettre les biens criminels à l'abri des poursuites.

Parmi les stratégies à mettre en œuvre plusieurs instances spécialisées internationales et européennes, notamment l'UE et le Conseil de l'Europe, ont identifié les IFC comme une composante essentielle de la stratégie de lutte contre la criminalité organisée. La principale source opérationnelle en matière d'IFC figure dans les recommandations du GAFI révisées en 2012. La définition des IFC figurant dans la note interprétative de la recommandation 30 et le document d'orientation de juin 2012. Dans ses rapports SOCTA de 2017, sur la menace constituée par la criminalité organisée transnationale, EUROPOL met en évidence que les connaissances parcellaires sur les mécanismes et acteurs impliqués dans le blanchiment de capitaux constituent une lacune substantielle dans la lutte contre les groupes criminels organisés transnationaux et que le renseignement financier est insuffisamment exploité.

Cette formation répond aux besoins ainsi identifiés au plus haut niveau européen en transmettant à des praticiens des services répressifs français et européens, les connaissances de base pour dépister l'argent sale, afin d'aboutir à une confiscation judiciaire. En effet, l'IFC porte simultanément sur l'infraction qui a généré les profits illicites et sur les flux financiers. Les informations financières collectées dans le cadre de cette enquête serviront à prouver l'infraction. Elle permet ainsi d'identifier les produits du délit, de les geler pour éviter leur disparition ou leur injection dans l'économie légale ou pour servir à commettre d'autres infractions.

Cette définition est extrêmement importante parce qu'elle sert de base à l'évaluation des actions menées par les États, conduite notamment par le GAFI et MONEYVAL. L'investigation financière est une investigation parallèle et proactive, permettant d'associer l'expertise policière et financière dans une approche complémentaire de manière à garantir que les infractions font l'objet d'une enquête exhaustive.

Parallèle, l'investigation financière porte simultanément sur l'infraction qui a généré les profits illicites et sur les flux financiers. Les informations financières collectées dans le cadre de cette enquête serviront à prouver l'infraction. Proactive, cette forme d'enquête permet d'identifier les produits du délit, de les geler pour éviter leur disparition ou leur injection dans l'économie légale ou pour servir à commettre d'autres infractions.

Objectifs généraux et spécifiques

Le projet porté par le CEIFAC vise à mettre en œuvre la recommandation du GAFI en proposant une action de formation à destination des enquêteurs spécialisés des États membres de l'UE. Celle-ci permettra aux auditeurs de mettre en œuvre une investigation financière, dans un contexte européen, dans le but :

1. d'identifier l'ampleur de réseaux criminels et/ou le degré de criminalité ;
2. d'identifier et de dépister le produit du crime, les fonds terroristes et tout autre bien soumis ou susceptible d'être soumis à confiscation ;
3. d'établir des preuves susceptibles d'être produites dans des procédures pénales ;
4. de dépasser les obstacles linguistiques pour mettre en œuvre les IF de manière efficace dans un contexte de coopération policière européenne ;
5. de renforcer la connaissance mutuelle en vue de contribuer à une culture commune en matière d'investigations financières.

Pour atteindre ces objectifs et réaliser le projet tel qu'il a été défini, le CEIFAC a mis en place une stratégie qui se décline en trois points.

I. Former à des techniques européennes d'investigation financière et d'analyse financière criminelles

À chaque session de formation ouverte, le CEIFAC a vocation à former un fonctionnaire par État membre de l'Union européenne : policiers, gendarmes, magistrats ou douaniers, soit une trentaine de stagiaires par session.

Les enseignements, en e-learning ou en présentiels, sont dispensés par des intervenants européens à la fois universitaires ou issus des autorités de police ou de justices, garantissant ainsi une formation de qualité et en phase avec les progrès techniques dans le domaine qui rend possible un essaimage de techniques communes efficaces et harmonisées dans toute l'UE.

De 2016 à 2019, 6 sessions de formation (2 par an) ont accueilli 30 auditeurs (15 français et 15 européens). Le CEIFAC a également organisé une conférence de synthèse en février 2019, conférence qui a eu pour objet de mettre en exergue les obstacles persistants en matière d'investigations financières.

Chaque session de formation s'achève avec une conférence/table ronde thématique accueillant des acteurs de premier plan des services répressifs, de la justice et du monde académique. Ces conférences sont ouvertes au public et à la presse et, tout en participant à la formation des auditeurs, permet la diffusion de la réflexion développée par l'équipe de recherche du CEIFAC.

II. Un outil commun pour une meilleure connaissance des phénomènes criminels

En termes de recherche, le CEIFAC a notamment pour objectif de créer une « référothèque », base de données informatique qui permet d'assurer, à l'échelle européenne, la collecte et l'analyse des informations en open source utiles aux investigations financières et à l'analyse financière criminelle au sein de l'Union européenne. Cette base de données a également pour finalité la constitution d'un centre de connaissances qui centralisera les bonnes pratiques en matière d'investigations économiques et financières, et l'élaboration des typologies des différents phénomènes criminels de nature économique et financière. Disponible en accès restreint, la référothèque offre aux forces de poursuite des États membres, un outil pour accéder à une meilleure connaissance des phénomènes criminels contre lesquels ils luttent.

Le CEIFAC s'appuie sur les compétences de l'équipe de recherche du Groupe de recherches actions sur la criminalité organisée (GRASCO), au sein de l'Unité Mixte de Recherche Droit Religion-Entreprise-Société (Université de Strasbourg/CNRS). Cette équipe, composée de docteurs en droit et placée sous la direction pédagogique de la directrice du laboratoire, Madame Chantal Cutajar, développe un programme de recherche et diffuse le fruit de leur réflexion ainsi que les pistes envisagées pour lutter contre la délinquance organisée via des parutions périodiques dans des revues et journaux spécialisés.

A l'occasion du programme de recherche, l'équipe propose à chaque session de formation en présentiel, un colloque thématique, ouvert au public et destiné à faire la lumière sur une question d'actualité. Le cycle en cours, dédié aux aspects cyber de la lutte contre la délinquance financière, se compose d'une conférence thématique, de trois colloques thématiques et d'une conférence synthèse (entre octobre 2019 et juin 2021). A l'issue de chaque colloque est publié un « Cahier du CEIFAC », somme de la réflexion des intervenants et un ouvrage sera rédigé en fin de cycle et diffusé à l'ensemble de la communauté universitaire, aux partenaires et au grand public.

Colloques du cycle « Cyber » :

- Jeudi 13 juin 2019 : « Le renseignement financier par EUROPOL : Bilan et perspectives »
- Jeudi 24 octobre 2019 : « Cryptomonnaies et blockchains : quelles perspectives ? »

- Mercredi 14 octobre 2020 : Conférence « Criminalité organisée et COVID-19 »
- Jeudi 15 octobre 2020 : « Cybercrime : Lutte contre les ransomwares, le phishing, le vol d'identité et autres infractions cyber »
- Vendredi 10 juin 2021 : « Jeux et paris en lignes : comment mieux lutter contre la corruption sportive et le blanchiment d'argent sale sur Internet »
- Vendredi 18 juin 2021 : conférence synthèse : « les nouveaux risques cyber »
-

III. Le CEIFAC ouvert sur la cité

Le CEIFAC contribue à ancrer Strasbourg dans sa vocation européenne et est ouvert sur la cité. Les conférences et colloques thématiques sont organisés pour donner au public des clés de lecture de la lutte contre le développement des réseaux criminels et les moyens de la soutenir.

Pour assurer une large transmission de ce travail de recherche, le CEIFAC diffuse au moyen d'un communiqué de presse et de l'envoi de cartons d'invitation, l'annonce du colloque ou de la conférence. Cette diffusion, faite auprès du public et de la communauté universitaire permet alors à chacun d'avoir accès à l'information et de participer aux débats, nourrissant alors la recherche (un moment d'échange avec les intervenants étant à chaque fois organisé). Les rencontres ont lieu, soit sur le campus de l'université, soit dans l'amphithéâtre de la bibliothèque universitaire, soit encore, dans un lieu plus proche du grand public, telle la salle de conférence d'une librairie, lieu de rencontre propice à la discussion, expérience que nous avons proposée au public strasbourgeois lors de l'organisation d'une conférence citoyenne axée sur « l'Europe de la justice » en octobre 2018. A cette occasion, le public a pu débattre de sujets tels que la lutte contre la corruption ou encore la protection des lanceurs d'alerte que sont les journalistes d'investigation.

Une pratique pédagogique alliant données théoriques et analyses pratiques

Le CEIFAC est hébergé au sein de l'UNISTRA, par l'Unité mixte de recherche (UMR) 7354, Droit, Religion, Entreprise, Société (DRES) laquelle il est rattaché administrativement.

Entièrement gratuite pour les auditeurs (voyages aller-retour du pays d'origine à STRASBOURG, hébergement et restauration et transport local (tramway et bus)). Les langues de travail sont le français et l'anglais. Une interprétation simultanée professionnelle est assurée vers ces deux langues.

La formation dispensée par le CEIFAC permet d'acquérir des savoirs et des savoir-faire ainsi que d'échanger de manière à faire émerger les meilleures pratiques. En alternant des cours en présentiel et des exercices pratiques, les auditeurs travaillent à partir de cas concrets tirés de situations réelles déroulant une investigation financière (IF), de son ouverture à sa clôture.

Lors de la phase de formation présentielle, les auditeurs travaillent en groupe configurés de façon à intégrer en leur sein les divers profils intervenant dans les IF (enquêteurs des corps de Police, Gendarmerie et Douanes et autorités de poursuite). Il s'agit de confronter les auditeurs, quel que soit leur profil et de manière transversale, aux difficultés susceptibles d'être rencontrées dans le cadre d'une IF. Chaque auditeur sera mis en situation d'apporter sa contribution de manière à faire émerger les meilleures pratiques en matière d'IF.

Le travail d'enquête peut être freiné par une connaissance imparfaite des modes opératoires en matière de cybercriminalité, comportements en constante évolution dont l'ingénierie tend chaque jour à se perfectionner se transformant peu à peu en véritable méthodologie criminelle. Il est alors essentiel de disposer de supports de travail efficaces qui permettent l'amélioration du dispositif de lutte contre cette forme de délinquance, permettant aux autorités publiques de se battre à armes égales.

Dans une démarche d'efficience, le CEIFAC propose la création d'une « boîte à outils » de l'enquêteur.

Cette initiative s'intégrera dans le dispositif européen destiné à appliquer la stratégie de cybersécurité de l'Union[1] et de la nécessité d'assurer la cohérence entre ses différentes initiatives dans le combat contre cette délinquance impalpable qui gangrène l'ensemble du cyberespace et des échanges mondiaux. Dans cette démarche, en 2017, le Conseil de l'Europe a proposé la création d'une "Boîte à outils cyber diplomatique" présentée comme un document de réflexion commun sur une réponse diplomatique conjointe de l'UE préoccupée par la capacité et la volonté accrues d'acteurs étatiques et non étatiques à poursuivre leurs objectifs en menant des activités cyber malveillantes, dont la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence sont variables, L'Union européenne a à cœur d'améliorer la cyber résilience, notamment grâce à la mise en œuvre de la directive SRI et aux mécanismes de coopération opérationnelle qu'elle prévoit, et rappelle que les activités cyber malveillantes dirigées contre des systèmes d'information, tels qu'ils sont définis par le droit de l'Union, constituent une infraction pénale et que la réalisation d'enquêtes et l'engagement de poursuites effectives à l'égard de telles infractions restent un effort commun des États membres[2].

Cette « boîte » qui, tel un syllabus, se présentera dans un format dématérialisé permettra un accès aisé, et comportera plusieurs volets thématiques pour avoir une vision globale de la matière. L'enquêteur ou le magistrat en charge de l'affaire aura accès à de multiples infirmations, actualisées par l'ensemble des acteurs de la scène pénale avec pour finalité d'obtenir une lutte efficace, méthodique et harmonisée à travers l'Union européenne.

Plusieurs points doivent alors être abordés dans ce nouveau support de travail des enquêteurs.

[1] Doc. 12109/13.

[2] Projet de conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cyber malveillance ("boîte à outils cyber diplomatique"), n° 7923/2/17 REV 2, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/fr/pdf.

1. Un glossaire unifié et harmonisé relatif à la lutte contre les cyberinfractions

Tout d'abord, pour une meilleure poursuite des actes criminels, il est nécessaire de procéder à une identification de ces comportements et actions qui tomberont sous le coup de la loi pénale dans l'ensemble des pays membres de l'Union européenne.

Pour ce faire, il est impératif de procéder à une cartographie des risques et des vulnérabilités face aux cyber infractions, qu'elles soient constitutives d'actes de blanchiment des produits de l'activité criminelle, d'actes ou de tentatives de corruption, de vol d'identité, de phishing, de rançongiciel, …

a) Définir la cybercriminalité

Avant toute chose, il est indispensable d'utiliser une terminologie harmonisée que ce soit dans les textes officiels, les documents de travail ou encore les différents actes se rattachant à l'identification, la poursuite et la sanction des criminels. Les organismes européens tel qu'Europol, *Enisa*[3], ou encore le Conseil de l'Europe devraient être en capacité d'utiliser les mêmes définitions à partir d'un glossaire qui soit disponible en plusieurs langues. En effet, bon nombre d'instances nationales, européennes ou internationales mettent à la disposition du public un glossaire. Malheureusement, la plupart d'entre eux est en langue anglaise et ne comporte aucune option de traduction fiable et fidèle aux termes techniques utilisés[4].

Une terminologie unifiée des termes permettra de circonscrire de façon claire le domaine d'intervention de la justice répressive. En suivant les textes européens et nationaux, la cybercriminalité couvre alors deux domaines différents et complémentaires, à savoir : l'ensemble des infractions spécifiques à Internet, pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit, par exemple les atteintes aux systèmes de traitements automatisés des données, les infractions en matière de fichiers ou de traitement informatique ou encore le domaine de la cryptologie : il s'agit d'infractions nouvelles spécifiques à Internet, relevant du piratage informatique, c'est-à-dire l'intrusion non autorisée dans les systèmes informatiques et le sabotage informatique de ceux-ci ; ou

[3] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary?tab=articles.

[4] Par exemple : Le *Law Enforcement Cyber Center* (LECC) est conçu pour aider les chefs de police, les shérifs, les commandants, les patrouilleurs, les enquêteurs médico-légaux numériques, les détectives et les procureurs qui enquêtent et préviennent les crimes impliquant la technologie. Son site Internet propose un glossaire bien construit, complet, mais uniquement en anglais (https://www.iacpcybercenter.org/resources-2/glossary/). Pour sa part, l'ANSSI propose également un glossaire dédié à son domaine d'expertise, glossaire en français (https://www.ssi.gouv.fr/entreprise/glossaire/a/).

encore des infractions de droit commun dont Internet permet la commission : il s'agit dans ce cas de formes traditionnelles de criminalité ou d'infractions de droit commun préexistant à Internet, mais qui se sont développées grâce à lui, la pédopornographie par exemple[5].

Il est à relever que le sujet, source de la réflexion ne fait l'objet d'aucune définition commune, occasionnant ab initio une insatisfaction et un malaise juridique. En effet, pour être efficace, le droit a besoin de règles claires et de socles stables que l'on trouve dans les définitions des termes, objets de la loi pénale. Dans ce domaine en constante évolution et touchant l'ensemble des membres de la société mondiale, seuls des critères récurrents ont pu être identifiés. Ainsi, cette forme de délinquance protéiforme se caractérise comme étant une forme de criminalité organisée, mondialisée et transnationale par nature qui exige une coopération européenne, voire internationale poussée[6].

Pour en définir les contours, il est ensuite indispensable de se référer au seul texte européen commun à tous et contraignant, la « Convention sur la cybercriminalité » de Budapest, recelant les lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, et faisant office de cadre pour la coopération internationale contre la cybercriminalité parmi les États parties. Complétée par le Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, la Convention comporte en son article premier l'ensemble des terminologies utiles à la matière. S'y trouvent ainsi définis les expressions « système informatiques », « données informatiques » et « fournisseur de service » ou encore « données relatives au trafic ». Mais, même si elle fait expressément référence à la « cybercriminalité » dès son Préambule, il n'est fait aucune mention d'une quelconque définition de ce qu'est cette forme de délinquance. Notons tout de même que les auteurs donnent une série d'actes pour lesquels la convention trouve à s'appliquer (« prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan

[5] Sénat, rapport d'information n° 613 (2019-2020) de Mme Sophie JOISSAINS et M. Jacques BIGOT, « Cybercriminalité : un défi à relever aux niveaux national et européen », http://www.senat.fr/rap/r19-613/r19-613_mono.html.

[6] Sénat, rapport d'information n° 613 (2019-2020) de Mme Sophie JOISSAINS et M. Jacques BIGOT, « Cybercriminalité : un défi à relever aux niveaux national et européen », http://www.senat.fr/rap/r19-613/r19-613_mono.html.

national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable »[7]).

b) Définir les infractions et terminologies de la matière

Après avoir défini la matière, son domaine de compétence, il semble indispensable de procéder à la définition des termes importants du sujet, particulièrement des infractions qui s'y rattachent.

Ainsi, en suivant les directives européennes applicables en la matière, il sera préférable d'adopter des expressions telles que « cyberattaquants », « cyberdélinquants » ou encore « cybercriminels » plutôt que la dénomination de *hackers*.

Concernant la définition des infractions spécifiques, les experts qui sont intervenus lors de la conférence synthèse proposent de laisser à l'Union le soin de poser des définitions communes à l'ensemble de la communauté. Il sera alors indispensable de déterminer une définition unique des comportements tels que : le rançongiciel[8], l'hameçonnage[9], le vol de données ou encore le vol d'identité[10]. Cette approche permettra alors que l'ensemble des acteurs de la scène pénale parlent de concert en faisant usage des mêmes définitions. Cette position participera alors à l'effort de cohérence, de clarté et de stabilité tant souhaité par l'Union européenne.

[7] Convention de Budapest, Préambule, https://rm.coe.int/168008156d.

[8] Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement (https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/).

[9] L 'hameçonnage (phishing en anglais) est un néologisme québécois créé en avril 2004 par l'Office québécois de la langue française. L'infraction consiste en une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc. Le but recherché est de voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

[10] La liste proposée ici ne se veut pas exhaustive afin de pouvoir laisser toute latitude aux experts européens de déterminer la liste des infractions qui méritent une harmonisation à l'échelle européenne.

2. La traduction juridique des comportements criminels

La plupart des cyberattaques commises ces dernières années présentent des points communs, des agissements tels que l'on peut parler d'ingénierie criminelle qui se fonde sur des mécanismes de l'ingénierie sociale. Ce phénomène peut se définir comme « un ensemble de compétences, de méthodes et de techniques pluridisciplinaires » qui ont pour but de tirer profit des vulnérabilités humaines, grâce à la manipulation et à la persuasion[11]. Le cyberattaquant contourne alors l'ensemble des barrières techniques de sécurité d'un système et gagne la confiance de l'usager pour obtenir les informations ou commettre une action malveillante. Les malfaiteurs se basent alors sur l'ingénierie sociale et respectent une méthodologie criminelle qui suit un processus, des phases.

Dans la phase préparatoire, l'auteur de l'attaque va collecter un certain nombre d'informations, une tâche plus ou moins générique, puisque sa stratégie peut être massive, ciblée, voire très ciblée. A partir des résultats de sa recherche, l'attaquant va créer un prétexte, composé d'un personnage et d'une situation crédible. Puis, il doit sélectionner les outils techniques et psychologiques les plus adaptés à son scénario afin de développer un « rapport » avec sa cible, de courte, moyenne ou longue durée, qui peut être fondé sur des émotions négatives, comme la peur, ou encore positives, par exemple, à travers la séduction. Ce piratage du cerveau lui sert à introduire une requête à sa victime, qu'elle va accepter, facilitant l'obtention d'informations sensibles, un virement, un accès physique ou logique à un système, *etc.*, sans spécialement comprendre le caractère préjudiciable de sa réaction. La requête permet le passage à la phase opérationnelle, dans laquelle nous constatons l'exécution de l'attaque et puis l'exfiltration de son auteur, lorsqu'il trouve un moyen de couper la communication sans être démasqué.

Le ***phishing* ou hameçonnage** et ses variantes représentent des procédés dans lesquels le cyberattaquant envoie un message non sollicité à sa cible, en se faisant passer pour un tiers de confiance afin d'introduire le prétexte qui lui permettra de l'inciter à communiquer des informations confidentielles, à travers un vecteur, en apparence légitime, mais contenant un logiciel malveillant. Nous parlons de *spear-phishing* et de *whaling* pour des faits plus ciblés et sophistiqués ; de *vishing*, lorsque le message est transmis par un appel téléphonique ou *VoIP* ; et de *smishing* en cas d'envoi par SMS.

[11] D. GROSS, L'ingénierie sociale : la prise en compte du facteur humain dans la cybercriminalité, thèse de doctorat soutenue le 8 juillet 2019, université de Strasbourg.

Il est intéressant de constater un grand nombre d'escroqueries présentent des modes opératoires identiques, à savoir créer un personnage qui va solliciter le transfert des sommes d'argent par avance à sa victime ou bien des informations sensibles. Les arnaques du type « 419 » ou par « avance de frais » sont les plus connues (citons par exemple, le fameux prince ou héritier). En général, l'escroquerie repose sur une combinaison d'émotions avec une promesse de gains potentiels plutôt que sur des outils techniques.

Il existe également des variantes de ces manipulations plus ou moins sophistiquées, comme les arnaques aux sentiments, des fausses offres d'emploi, de prêts et d'investissements. Il faut mentionner les escroqueries aux crypto-actifs puisque ces derniers, ne constituent pas seulement un moyen de paiement ou de blanchiment, mais un outil détourné par les malfaiteurs visant leurs détenteurs, investisseurs, intermédiaires. Dans de tels mécanismes frauduleux interviennent de faux prestataires, de fausses plates formes de placement et d'échanges de cryptomonnaies qui, par exemple, récupèrent les sommes et disparaissent sans laisser de traces physiques ou numériques.

Le ***cryptojacking*** est une attaque qui permet aux malfaiteurs à la suite de l'installation d'un logiciel malveillant, d'utiliser à l'insu de la victime la puissance de calcul de son ordinateur pour le minage de crypto-actifs.

L'**arnaque au faux support technique** a évolué, notamment à partir de la démocratisation du télétravail. Il s'agit de provoquer chez la victime, par message écrit ou un appel, un sentiment de panique face à un problème technique dans son dispositif et l'inciter à contacter un support technique, qui finira par lui demander de payer pour le dépannage, acheter des produits, lui envoyer ses identifiants, voire prendre l'accès à distance au dispositif.

Soulignons, par ailleurs, l'utilisation frauduleuse des cartes bancaires mais non seulement à partir du phishing puisque la copie et la commercialisation des données bancaires volées à travers les techniques de *skimming*, anciennes et nouvelles, ainsi que de *carding* sont toujours d'actualité.

Les **fraudes aux faux ordres de virement**, avec ses variantes, l'arnaque au président et celle du changement de RIB du fournisseur, sont commises en ciblant un employé, souvent responsable de la comptabilité, qui est incité à effectuer le virement d'une somme considérable d'argent, appartenant à la personne morale, généralement vers un compte situé à l'étranger, à la suite d'un problème de compte, à la délocalisation d'un service, ou bien, dans le cadre d'une opération urgente et confidentielle.

Parmi les différents types de *malware* qui touchent les systèmes informatiques, les **rançongiciels** font actuellement des ravages. Ces logiciels malveillants servent aux malfaiteurs à extorquer les victimes, en bloquant leurs dispositifs ou en chiffrant leurs fichiers, afin

de leur demander une rançon, même si son règlement ne peut pas assurer l'accessibilité aux contenus affectés. Bien au contraire, le paiement est fortement déconseillé car il nourrit l'écosystème criminel et même les cyberassurances sont en train de revoir leurs politiques de remboursement. De plus, il arrive que les cyberattaquants menacent aux victimes de diffuser au public leurs données confidentielles sur Internet.

Force est de constater que la plupart de ces faits sont commis à partir des usurpations d'identité, infraction qui peut servir à effectuer des virements ou passer des commandes de manière frauduleuse, et devenir aussi un vecteur pour nuire à la réputation d'une personne physique ou morale, via les réseaux sociaux.

Dans un grand nombre des cas étudiés, des données à forte valeur sont en jeu ainsi que leur bonne maîtrise, dont l'importance devient évidente au regard du RGPD, situation qui est largement exploitée par les cybercriminels.

Force est de constater une industrialisation de la cybercriminalité car, tous les mécanismes que nous venons de mentionner sont réalisables grâce aux produits et services proposés sur le *Dark Web*, la face cachée du *Web*, dans laquelle il est possible de naviguer avec plus de liberté, en se procurant des moyens d'anonymisation, sans oublier le recours à des services de messagerie chiffrée et aux hébergeurs qui tolèrent des contenus pour le moins reprochables, en exploitant des failles juridiques qui les aident à placer leurs serveurs dans des juridictions favorables ou encore des vulnérabilités techniques de services légitimes qui ne sont pas correctement sécurisés.

Les cyberattaquants se rendent ainsi sur le *Dark Web*, pour acheter des données, des outils et solliciter des services afin de planifier leurs attaques. Puis, à la fin de chaque cycle d'attaques pour monétiser l'information ou blanchir leur butin.

Toutes ces pratiques sont fondamentales pour faire tourner l'économie souterraine liée à la cybercriminalité et doivent nécessairement s'adapter aux évolutions technologiques et juridiques. C'est pourquoi, nous devons identifier les tendances.

La pandémie de la COVID-19 a multiplié le nombre de faits présentés, suite à plusieurs facteurs : l'augmentation de la surface d'attaque des réseaux cybercriminels ; l'incertitude de la population isolée mais hyper connectée partageant des contenus anxiogènes ; le travail à distance sans formation au préalable, entraînant des échanges en permanence à partir de réseaux et dispositifs domestiques non sécurisés, entre autres. Le confinement a prouvé l'opportunisme des cybercriminels qui ont modifié leurs prétextes, désormais basés sur : des commandes en ligne ; des problèmes à résoudre par les télétravailleurs ; des aides sociales ou des dons inexistants ; faux permis

de circulation ; faux tests de Covid ; faux masques ; faux vaccins et certificats de vaccination ; téléchargement d'applications malveillantes, *etc*.

En observant les statistiques publiées récemment par la plateforme française cybermalveillance[12], en ce qui concerne les demandes d'assistance aux victimes, (particuliers, entreprises, associations, collectivités, administrations) durant l'année 2020, nous pouvons confirmer tous nos propos. La crise économique liée à cette pandémie est évidemment un terrain fertile pour des nouveaux scenarii.

Parallèlement, il est possible de constater l'augmentation des attaques de *Sim swapping*, dans lesquelles le cyberattaquant va obtenir des données personnelles de sa cible, contacter et duper l'opérateur de sa ligne téléphonique pour demander la portabilité du numéro afin de pouvoir prendre le contrôle de sa ligne avec une carte Sim qu'il détient afin de recevoir les appels et sms adressés à la victime, y compris les codes à usage unique et le double facteur d'authentification.

En outre, la diversification des objets connectés nous rend encore plus fragiles, il s'agit d'un écosystème très vaste mais risqué si l'utilisateur et les fournisseurs des services liés aux objets connectés (développement, production, support, maintien) ne prennent pas suffisamment en compte les mesures de cybersécurité adéquates dès leur conception. Ces équipements sont vulnérables à des failles au niveau du hardware et du software, un usage incorrect et même un manque de mise à jour peut très facilement donner lieu à une infection avec toutes ses conséquences : vol de données, botnets, espionnage, rançongiciel, voire la mise en danger des personnes.

Il convient également évoquer l'emploi du ***deepfake*** dans le cadre de certaines attaques telles que des usurpations d'identité, *fake news*, *phishing* et arnaques au président. La fabrication de faux contenus multimédia, notamment à partir des images ou vidéos préexistantes à l'aide du *deep learning* est vraiment dangereuse car son usage astucieux assure la crédibilité nécessaire du personnage joué par l'attaquant devant sa victime.

Enfin, le ***jackpotting*** est une attaque physique et logique, pour certains inédite, car il faut brancher un câble dans un modèle spécifique de distributeur de billets vulnérable, pour le connecter à un ordinateur, afin de prendre le contrôle de l'automate, accéder aux données du calculateur ou bien l'infecter avec un logiciel malveillant, et ensuite, à distance, le forcer à « cracher » des billets, dans le but de le vider totalement ou partiellement.

[12] https://www.cybermalveillance.gouv.fr/.

À partir de cette analyse phénoménologique, il devient nécessaire de réfléchir aux obstacles dans la lutte contre la cybercriminalité, non seulement du point de vue répressif mais aussi préventif et spécialement en ce qui concerne l'aide aux cybervictimes.

La criminalité visant les **systèmes de traitement automatisés de données** (STAD) est sanctionnée pénalement par des incriminations et des circonstances aggravantes spécifiques.

En pratique, la cybercriminalité correspond à une liste d'infractions, ainsi qu'à une façon d'opérer. Les infractions d'atteintes aux STAD sont prévues aux articles 323-1 et suivants du Code pénal français et répriment :

- le fait d'accéder ou de se maintenir frauduleusement dans un STAD ;
- le chiffrement des données du système compromis par le rançongiciel constitue le fait d'entraver ou de fausser le fonctionnement d'un STAD;
- le fait d'introduire frauduleusement des données dans un STAD ;
- le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée, conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions.

Les qualifications classiques peuvent être aussi établies comme l'escroquerie notamment en bande organisée, l'abus de confiance, le blanchiment simple ou en bande organisée (C. pénal français, art. 324-1) permettent, par ailleurs, de réprimer bon nombre d'actes frauduleux dans leur dimension numérique.

La demande de rançon est qualifiée d'extorsion ou de tentative d'extorsion (312-1 du code pénal français). Dans une procédure de *jackpotting* d'envergure sur l'ensemble du territoire national, les infractions suivantes ont pu être retenues à l'encontre des cybermalfaiteurs : l'accès frauduleux dans un système de traitement automatisé de données avec la circonstance qu'il en est résulté une altération du système; maintien frauduleux dans un système de traitement automatisé de données avec la circonstance qu'il en est résulté une altération du système; entrave au fonctionnement d'un système de traitement automatisé de données; introduction frauduleuse de données dans un système de traitement automatisé; vol en bande organisée; une atteinte au fonctionnement d'un système de traitement automatisé de données; association de malfaiteur en vue de commettre un crime.

Les incriminations susceptibles d'être retenues à l'encontre de l'auteur du *phishing*. A défaut d'une incrimination *ad hoc*, plusieurs textes et qualifications sont susceptibles de s'appliquer.

Usage d'une fausse identité. En premier lieu, l'auteur du *phishing* emprunte un faux nom et une fausse qualité pour se faire passer pour un prestataire de services sur actifs numériques réel. Deux infractions sont susceptibles de s'appliquer : l'infraction consistant à « prendre le nom d'un tiers » et l'infraction d'« usurpation d'identité numérique ».

La première infraction implique un risque de poursuites pénales à l'encontre de la personne dont l'identité a été usurpée, condition qui n'est pas requise en ce qui concerne l'infraction d'usurpation d'identité. Or, dans le cadre d'un *phishing*, l'usurpation d'identité n'est pas toujours réalisée dans des circonstances qui déterminent des poursuites pénales contre le tiers. Dès lors, l'infraction d'usurpation d'identité numérique est plus adaptée au phishing. En effet, selon la législation française, l'article 226-4-1 du code pénal réprime le fait « d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ». L'infraction d'usurpation d'identité en ligne, intégrée au code pénal depuis la loi LOPPSI 2[13], prévoit une peine an d'emprisonnement et de 15 000 € d'amende.

Contrefaçon. Lorsque l'auteur du phishing reproduit le site web ou l'application mobile d'une société existante, il est susceptible d'être incriminé pour contrefaçon de marque (logos, signes, emblèmes…), réprimé par l'article L. 713-2 du code de la propriété intellectuelle. L'article L. 713- 3 du même code prévoit une interdiction de tirer indûment profit du caractère distinctif ou de la renommée de la marque.

Collecte illicite de données personnelles. L'objectif de l'auteur du phishing est de soustraire à la victime ses données personnelles, en particulier ses codes d'accès à la véritable application qu'il imite, ou encore la phrase secrète de la victime, directement liée à ses clés cryptographiques privées.

Or, l'article 226-18 du code pénal, intégré par la loi Informatique et Libertés 46, sanctionne le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite de cinq ans d'emprisonnement et 300 000 € d'amende.

Cyber-escroquerie. L'auteur du *phishing* fait usage d'un faux nom et d'une fausse qualité afin de tromper l'utilisateur d'un service sur actifs numériques et de le déterminer à entrer ses codes d'accès ou sa phrase secrète. A la différence d'un vol, la remise d'un bien dans le cadre de l'escroquerie peut consister en un bien immatériel. Dès lors, les conditions nécessaires à l'escroquerie sont remplies. À titre d'exemple, l'auteur d'un *phishing* se faisant passer pour un banquier a été condamné pour escroquerie. Cette infraction est punie de

[13] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n°0062 du 15 mars 2011.

cinq ans d'emprisonnement et de 375 000 euros d'amende. Par ailleurs, selon les circonstances, la pratique du *phishing* peut donner lieu à un *spamming* ou à l'usage frauduleux d'un moyen de paiement.

Une politique pénale réaffirmée doit être renforcée et la chancellerie (DACG) s'y emploie en développant des outils pédagogiques sous formes de fiches réflexes à destination des magistrats. Il faut souligner également la création de la nouvelle compétence du tribunal judiciaire de Paris, la juridiction nationale de lutte contre la criminalité organisée (Junalco), en mars 2019 dont dépend désormais la section J3 spécifiquement dédiée à la cybercriminalité. On assiste à une certaine clarification du rôle des acteurs judiciaires qui pourra peut- être encore évoluer suite à la mise en place du parquet européen depuis le 1er juin 2021 qui a en charge des fraudes commises au préjudice de l'UE, ces infractions d'envergure étant de plus en plus numériques.

Dès à présent, on note que la plupart des affaires de cybercriminalité d'envergure ont une dimension internationale et que le mandat d'arrêt européen[14] ou encore le mécanisme de la décision d'enquête européenne[15] constituent des outils efficaces de lutte et d'interpellation des cybercriminels.

Il s'agit aussi de clarifier le rôle des acteurs judiciaires, rôle qui évoluera encore avec la mise en place du parquet européen depuis le 1er juin 2021. En charge des fraudes commises au préjudice de l'UE, le Parquet européen pourra aussi à l'avenir contribuer à renforcer la lutte contre la cybercriminalité d'envergure.

Quid alors de l'arsenal juridique en matière cyber et notamment la **Convention de Budapest**[16] ?

En termes de criminalité organisée et lorsqu'il s'agit de correspondances électroniques stockées, le code de procédure pénale français prévoit, avec autorisation du magistrat, la possibilité de perquisitionner à distance et à l'insu de la personne visée. Malheureusement dès lors que les données sont stockées dans un pays n'ayant pas ratifié la convention de Budapest, les enquêteurs se retrouvent privés de cette véritable arme judiciaire. La procédure est essentielle également car elle permet d'accéder à la preuve numérique qu'il convient de sécuriser et de recueillir dans des conditions loyales. Il faut souligner que l'adoption du deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques en novembre

[14] Décisions-cadre 2002/584/JAI relative au mandat d'arrêt européen et aux procédures de remise entre les pays de l'UE.
[15] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, OJ L 130, 1.5.2014, p. 1–36.
[16] https://www.coe.int/fr/web/cybercrime/the-budapest-convention.

2021 sera suivie de son ouverture à la signature en mai 2022. Sa ratification est, à n'en pas douter, urgente car cet instrument va permettre de renforcer la lutte contre ce fléau[17].

Recommandations

1. Renforcer l'impact de la Convention de Budapest.
2. Promouvoir son rayonnement dans les pays non-membres du Conseil de l'Europe et n'ayant pas encore ratifié le texte et les protocoles additionnels.
3. Donner une définition harmonisée de la cybercriminalité.
4. Proposer un glossaire des termes propres à la matière, glossaire disponible et fidèle dans toutes les langues européennes.
5. Pour l'année 2022, faire que la lutte contre la cybercriminalité soit proclamée grande cause nationale, européenne et internationale.

[17] Le "Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques" a été approuvé par le Comité des ministres le 17 novembre 2021. Il a été préparé par le Comité de la Convention sur la cybercriminalité (T-CY) entre septembre 2017 et mai 2021. Plus de quatre-vingt-dix sessions de la plénière de rédaction du protocole T-CY, du groupe de rédaction et des sous-groupes, ainsi que six cycles de consultations des parties prenantes ont eu lieu au cours de cette période. Il est prévu que ce protocole soit ouvert à la signature en mai 2022. https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group.

3. Renforcer les capacités opérationnelles des enquêteurs européens

a) Renforcer la formation des enquêteurs européens

Le CEIFAC est avant tout l'unique centre de formation dédié aux investigations financières, à l'analyse criminelle financière avec des modules renforcés en cybercriminalité à l'échelle européenne. Composante active de l'Université de Strasbourg, le CEIFAC a pour mission de former les membres des forces de l'ordre et de la magistrature des États membres de l'Union européenne. Fort de plus de 440 acteurs formés entre 2013 et 2021, le CEIFAC s'inscrit dans une offre de formation plus grande qui est abritée par différents pôles universitaires dirigés par Mme Chantal Cutajar, Directrice générale du CEIFAC et maître de conférences HDR rattachée à l'Université de Strasbourg.

Par exemple, en partenariat avec l'Université de Strasbourg, capitale européenne, a été créé un Master II professionnalisant intitulé « investigations financières à l'échelle européenne ». Cette nouvelle offre de formation a été pensée et construite pour répondre aux besoins et aux impératifs liés au public visé en proposant une formation entièrement en distanciel, basée sur l'étude de cas issus de la pratique, questionnant la coopération à l'échelle européenne et faisant la place belle aux aspects liés à la cybercriminalité.

Par ailleurs, dans le but de proposer une formation globale et graduée des enquêteurs en matière de délinquance financière, particulièrement en matière de cyberdélinquance, a été mise en place une formation diplômante de niveau 7 ainsi qu'une certification. Cette formation fait suite au constat qu'il n'existe actuellement que des formations visant à apprendre aux acteurs à se protéger ou/et à se défendre, mais aucune offre ne permet d'effectuer une analyse complète des systèmes pour déterminer où se situent les éléments sensibles et permettre ainsi de les anticiper, de les éluder ou de les résoudre. La nouvelle formation permet d'acquérir des connaissances dans les domaines touchant à la recherche et l'analyse d'informations au sein des systèmes numériques. Elle permet non seulement de former des professionnels destinés au service de l'État chargé des poursuites mais également aux organisations privées afin de déterminer la provenance de malveillances sur leurs systèmes informatiques.

Enfin, il est important de noter qu'il existe une grande disparité en matière de dissémination des techniques à appliquer entre les pays européens, c'est pourquoi, il serait nécessaire de mettre en place ce type de dispositif de formation destiné à uniformiser les actions et échanges au niveau européen.

b) La spécificité des crypto-actifs

En juin 2019, lors de la réunion plénière du Groupe d'action financière (GAFI), les États membres avaient adopté de nouvelles normes communes applicables aux actifs numériques et aux prestataires de services numériques (recommandation 15 et 16) avec pour visée l'application de standards contre le blanchiment de capitaux et le financement du terrorisme.

Le 28 octobre, le GAFI a publié ses lignes directrices 2021 sur les standards en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme applicables aux crypto-actifs. Cette mise à jour des lignes directrices fait suite au constat fait par l'institution des « lacunes » dans la mise en œuvre de la précédente réglementation en la matière. En effet, le GAFI a établi qu'il était nécessaire d'« intégrer et de remplacer les orientations » édictées en 2019 (protocole de déclaration des *cryptoexchanges*, « *Travel Rule* »), ces dernières n'ayant pas été transposées ou appliquées de manière satisfaisante dans certaines juridictions. A cette occasion, le GAFI a actualisé sa définition des « actifs virtuels » et celle des fournisseurs de services d'actifs virtuels (VASP), avertissant qu'ils « ne devraient pas exister de cas où un actif financier pertinent (ne soit pas) couvert par les normes du GAFI »[18].

Suivant les recommandations du GAFI, pour que les enquêteurs puissent agir dans les meilleures conditions, le CEIFAC mettra en place en 2022, une formation dédiée aux actifs virtuels. Cette formation, très technique, sera dispensée dans le cadre des formations thématiques visant à renforcer l'expertise des membres des forces de l'ordre et de la justice européenne. Cette formation d'une journée sera inscrite au catalogue de formation du CEIFAC à la rentrée universitaire 2023 et proposée à l'ensemble des acteurs de la scène répressive européenne.

[18] Voici quelques autres points clés de la directive mise à jour :
Une section sur les NFT est incluse, mais il semble qu'il ne s'agit que d'une ébauche : il est mentionné que certains NFT peuvent être qualifiés de crypto-actifs, cependant "les pays devraient [...] envisager l'application des normes du GAFI aux NFT au cas par cas."

- Les applications DeFi elles-mêmes ne sont pas des VASP, mais "les créateurs, les propriétaires et les opérateurs ou certaines autres personnes qui maintiennent un contrôle ou une influence suffisante sur les protocoles DeFi" peuvent l'être - et peuvent avoir besoin d'obtenir des permis d'exploitation.
- En ce qui concerne les transactions P2P, l'organisme a noté que ces transactions peuvent comporter des "risques" similaires à ceux des cryptomonnaies. Il est écrit : "Bien que le GAFI n'ait pas observé de tendance distincte vers une utilisation accrue des transactions P2P jusqu'à présent, des risques potentiels liés à une augmentation des transactions de ce type pour éviter les réglementations/supervisions existent, à mesure que davantage de juridictions mettent en œuvre les normes du GAFI et supervisent les VASP."
  - Le GAFI ne considère pas les organismes industriels autorégulateurs comme des organismes d'application appropriés.
  - Il est nécessaire de renforcer "le partage et la coopération entre" les "superviseurs de VASP" nationaux.

4. Envisager la création d'un parquet européen spécialisé en matière de cybercriminalité

a) Créer un parquet européen spécialisé dans la cybercriminalité suivant le modèle du parquet financier pour lutter contre les cyberattaques visant les institutions de l'Union européenne.

Chaque année, plusieurs milliards d'euros échappent au budget européen. Pour y remédier, 22 pays de l'Union européenne ont décidé de créer un Parquet européen qui vient d'entrer en fonction le 1er juin 2021. Organe indépendant de l'Union européenne chargé de rechercher, poursuivre et renvoyer en jugement les auteurs d'infractions pénales portant atteinte aux intérêts financiers de l'Union, le parquet européen est compétent en matière de fraude, de blanchiment, de corruption et de fraude transfrontière à la TVA[19]. Il s'agit d'un pas important vers l'instauration d'un espace commun de justice pénale dans l'UE.

Le sujet de la lutte contre la cybercriminalité imprègne progressivement les travaux européens, preuve en est que, pour la première fois, cette catégorie d'infractions est inscrite dans le texte de la directive 2018/1673 du Parlement européen et du Conseil en date du 23 octobre 2018, dite « Sixième directive anti-blanchiment »[20]. Composante d'un paquet législatif qui inclut le règlement (UE) 2018/1672 relatif aux contrôles de l'argent liquide entrant dans l'UE ou sortant, la directive de 2018 complète et renforce l'application de la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. La directive vient ainsi définir les infractions pénales et les sanctions dans le domaine du blanchiment d'argent en vue de faciliter la coopération policière et judiciaire entre les pays de l'UE en évitant que les criminels ne profitent de systèmes juridiques plus cléments ; elle vise à criminaliser le blanchiment d'argent lorsqu'il est commis intentionnellement et en sachant que les biens proviennent d'une activité criminelle et enfin, elle permet aux pays de l'UE d'ériger en infraction pénale le blanchiment d'argent lorsque l'auteur de l'infraction soupçonne ou aurait dû savoir que les biens proviennent d'une activité criminelle.

L'intégration des cyberinfractions dans le nouveau dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme peut alors constituer le levier d'une réflexion relative à l'élargissement des compétences du Parquet européen aux cyberattaques, particulièrement lorsqu'elles touchent les institutions européennes. Ces nouvelles attributions coïncideraient avec les nouveaux dispositifs mis en place au niveau européen, tout particulièrement en matière de coopération policière et judiciaire internationale,

[19] https://www.eppo.europa.eu/.

[20] Directive 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018 visant à lutter contre le blanchiment de capitaux au moyen du droit pénal, article 2, 1) v.

coopération indispensable qui se heurte encore à trop de lenteur[21]. L'adoption et l'entrée en vigueur de la convention de Budapest du Conseil de l'Europe a permis d'harmoniser les outils d'entraide judiciaire, faisant de la lutte contre la cybercriminalité une de ses priorités en intégrant au dispositif de lutte l'ensemble des acteurs de la scène pénale européenne, particulièrement les agences Europol et Eurojust qui voient progressivement leurs attributions respectives évoluer[22].

Par exemple, partant du constat de la constante évolution de ce phénomène criminel, considéré comme protéiforme et mouvant, Eurojust et le Conseil de l'Europe organisent des ateliers de travail sur la coopération internationale en matière de cybercriminalité : équipes communes d'enquête / enquêtes conjointes. Au cours d'ateliers ou de webinaires, en s'appuyant sur une nécessaire coopération internationale rapide et efficace entre les autorités de justice pénale des États pour qualifier les infractions, identifier les pouvoirs procéduraux à utiliser et les juridictions qui s'appliquent aux différentes activités illégales, les deux entités ont convenu d'unir leurs forces pour s'attaquer à ce problème, inter alia par le biais du renforcement des capacités[23].

Dans la construction d'une Europe de la justice[24] et étant donné l'impérieuse nécessité de voir s'organiser un dispositif de lutte efficace et global, il semble indispensable d'accroître les pouvoirs de cette toute nouvelle entité qui n'a pour autre mission que de défendre les intérêts financiers de l'Union européenne, que ces intérêts soient identifiés dans le monde physique ou dans le monde virtuel.

[21] https://www.senat.fr/presse/cp20200709d.html.

[22] Par exemple : le 21 septembre 2021, la justice annonçait le démantèlement et l'arrestation d'un groupe cybercriminel lors d'une opération menée par les polices italiennes et espagnoles, avec le soutien d'Europol et Eurojust, menant à 106 arrestations (https://www.zdnet.fr/actualites/cybercrime-106-arrestations-en-espagne-et-en-italie-39929535.htm).

[23] https://www.coe.int/fr/web/cybercrime/council-of-europe-and-eurojust-2021-annual-meeting-jits#{%22107800064%22:[0]}.

[24] Voir les recommandations issues du colloque organisée par le CEIFAC, « Quelle Europe de la justice voulons-nous ? », 28 octobre 2018, https://www.canalc2.tv/video/15217, www.ceifac.eu

b) Créer dans chaque État une formation juridictionnelle spécialisée comportant des membres du parquet et des magistrats du siège : imaginer une chaîne pénale complète dans chaque État membre, relais et interlocuteur privilégié de l'instance pénale européenne.

La création d'une chaîne pénale allant de l'enquêteur au magistrat devrait permettre d'assurer une cohérence et une fluidité dans l'administration de la justice. En effet, il a été relevé qu'en matière de cyberattaque, les cyberdélinquants bénéficient d'une défense efficace et de procédures qui peuvent être fragilisées juridiquement.

En France, la loi du 23 mars 2019 de programmation pour la justice uniformise certaines procédures ainsi que leur condition d'application. Les mesures nouvelles et spécifiquement en matière de techniques spéciales d'enquête (écoutes et géolocalisation, enquêtes sous pseudonyme, …) sont entrées en vigueur au 1er juin 2019 en France. Il faut cependant noter que le Conseil constitutionnel a refusé le recours automatique aux techniques citées précédemment ; jugées « particulièrement intrusives » (sonorisation, intrusion informatique, …), elles sont réservées à la délinquance organisée (hors interception des correspondances électroniques stockées).

Pour contrecarrer le jeu à somme nulle, il paraît indispensable de parvenir à une meilleure sécurisation des procédures. Dans cette optique, il serait intéressant de mettre en place une sorte d'échange entre les magistrats et les enquêteurs lesquels bénéficieraient d'un retour sur les actes qui ont fait l'objet de la nullité. Par la mise en place d'un mécanisme d'information à destination des enquêteurs, il serait alors possible d'éviter la redite d'erreurs et de prévenir toute action en nullité de la part des conseils juridiques des mis en cause dans une procédure répressive.

Il serait alors envisageable de mettre en place un protocole d'information et d'échange en organisant des réunions type de « feed-back » qui mettraient en synergie l'ensemble des acteurs du dossier. Ces réunions rassembleraient alors les magistrats du siège, du parquet et les enquêteurs autour d'une même table dans une visée commune d'amélioration des pratiques et de la maîtrise des éléments procéduraux. A l'issue de telles réunions, il serait intéressant que soient rédigées des notes à destination des services d'enquête, reprenant les causes de nullité soulevées lors des différentes phases du procès afin qu'elles puissent être évitées à l'avenir.

5. Favoriser la création d'un réseau européen d'enquêteurs criminels spécialisés

Par le développement de formations européennes telles que celles proposées par le CEIFAC qui mettent en synergie les représentants des forces de l'ordre et de la justice européenne.

L'échange d'informations et la coopération interservices et inter-états demeure la seule vraie réponse à l'expansion des phénomènes criminels. Alors que les délinquants ignorent les frontières, les forces de l'ordre restent empêchées dans leur action. Pour ce faire, seules des mises en contact régulier des différents acteurs permettent de constituer des réseaux d'échanges d'informations fiables. Ces mêmes réseaux sont alors également l'occasion pour les protagonistes de nourrir chacun et chacune des expériences propres à chaque entité, permettant de monter en compétence et d'accroître son savoir.

L'expérience du CEIFAC en la matière a su prouver que par la mise en synergie des différents représentants et acteurs européens, bon nombre d'enquêtes ont pu être, si non solutionnées, au moins facilitées. La synergie mise en place a permis l'identification et l'élaboration de méthodologies communes, de canaux de discussion et d'identification de points de contacts.

Il est donc indispensable de développer des rencontres entre les acteurs, des mises en synergie basées sur des thématiques dédiées au perfectionnement et à l'amélioration des échanges entre enquêteurs et magistrats européens, notamment dans le domaine très technique et perpétuellement en mouvement que sont les investigations forensiques concernant les cryptomonnaies, l'OSINT ou encore le Darknet.

Ces rencontres thématiques, organisées périodiquement auraient pour but de maintenir les représentants des forces de l'ordre à un niveau d'expertise leur permettant de rivaliser avec des techniques criminelles toujours plus élaborées.

Dans ce cadre, le CEIFAC propose d'organiser chaque année des sessions d'actualisation à destination de l'ensemble des acteurs de la scène pénale européenne. Dans cette tâche et afin de favoriser le développement de réseaux et de forums d'échanges entre enquêteurs et magistrats, le CEIFAC a déjà mis en place un forum de discussion ouvert sur le site du CEIFAC et accessible à toutes les personnes qui ont suivi la formation dispensée par la CEIFAC.

Recommandations

1. Identifier les points de contact nationaux, européens et internationaux.
2. Créer un parquet européen spécialisé dans la cybercriminalité suivant le modèle du parquet financier pour lutter contre les cyberattaques visant les institutions de l'Union européenne.
3. Créer une chaîne pénale compète dans chaque État membre, relais et interlocuteur privilégié de l'instance pénale européenne.
4. Améliorer les dispositifs de discussion et d'échange entre les acteurs de la chaîne pénale.
5. Développer et multiplier les offres de formations européennes telles que celles proposées par le CEIFAC qui mettent en synergie les représentants des forces de l'ordre et de la justice européenne.

6. La boîte à outils du cyber enquêteur

Une boite à outils disponible en plusieurs langues pour les Officiers de police judiciaire et les magistrats européens.

Il est proposé de créer une boîte à outils des acteurs de la scène répressive européenne.

Ce document « ressource », disponible dans les langues officielles de l'Union européenne, comportera un glossaire sur les modes opératoires, les définitions des infractions telles qu'édictées dans chaque pays et au niveau européen, les procédures adaptées au numérique, notamment pour l'accès aux données.

La boîte à outils recèlerait également une check-list destinée à guider l'enquêteur dans son investigation.

Le document a été créé par les soins de la police fédérale belge, plus particulièrement Grey Cauwelier, inspecteur Principal Spécialisé entre 2018 et 2020. L'édification de ce document a été réalisée à la suite de la participation de sa Division OCRC à un groupe de travail du Plan National de Sécurité (PNS) dans lequel une des priorités était la lutte contre la criminalité financière. Cette check-list a été contrôlée, vérifiée par plusieurs enquêteurs spécialisés EcoFin et validée par la communauté pénale du pays. Après avoir participé à une formation du CEPOL à Skopje, le rédacteur de ce document-support a fait quelques mises à jour concernant la législation européenne, actualisations qui devront être permanentes et régulières pour assurer l'efficacité du dispositif.

Après avoir donné une présentation à divers collègues (enquêteurs, magistrats et analystes stratégiques) faisant le même travail dans divers pays d'Europe et des Balkans ; nombreux de ceux-ci furent impressionnés et ont voulu prendre une initiative similaire dans leur pays et dans les services d'enquêtes nationaux.

Sur la base de cette expérience fructueuse, les intervenants à la conférence synthèse du CEIFAC ont considéré qu'il était indispensable de proposer un tel document afin que ce dernier puisse servir de base de travail pour l'ensemble de la communauté répressive européenne.

Il s'agit alors de développer une posture commune et une stratégie harmonisée pour les enquêteurs dans la lutte contre la délinquance financière transnationale.

Le but principal de cet outil est d'aider les enquêteurs à mener une enquête financière, qu'elle soit physique ou numérique.

Elle n'a pas pour but d'obliger les enquêteurs à effectuer l'enquête financière. Parfois, certaines possibilités de recherche sont négligées ou ne sont pas connues. Avec cette liste, les enquêteurs ont la possibilité de vérifier s'ils n'ont rien oublié.

Un prérequis reste toutefois à rappeler, il est, en effet, indispensable que l'on passe par une harmonisation des procédures, des conditions de perquisitions et d'analyses des données numériques, et a fortiori de tous éléments pouvant servir de preuve.

Exemple d'harmonisation indispensable dans le cadre des enquêtes transnationales : l'accès aux données de connexion et conditions d'exploitation des autres données. Pour étayer notre réflexion, prenons quelques exemples de législation européenne.

La législation tchèque impose que les fournisseurs disposent des données (sociétés de télécommunications = ISP - fournisseur de services Internet, ou IAP - fournisseur d'accès Internet) pendant une période de 6 mois. Avec l'accord du tribunal, l'accès aux données de connexion est ouvert aux organes actifs dans les procédures pénales, à la police de la République tchèque, aux services de renseignements, aux renseignements militaires et à la Banque nationale dans le but de contrôler le marché des capitaux. L'obligation de stocker des données de telle sorte est insérée dans la loi n° 127/2005 Coll. sur les communications électroniques (§ 97, paragraphe 3). La portée des données elles-mêmes est réglementée par le décret 357/2012 Coll. sur le stockage, la transmission et l'élimination des données opérationnelles et de localisation. Le renseignement militaire tchèque peut exploiter ses propres installations chez les fournisseurs de services de télécommunications conformément à la loi 289/2005 Coll. et à l'article 98a de la loi sur les communications électroniques depuis 2021 pour prévenir et détecter les cyberattaques et les menaces. Ces boîtes noires sont appelées "outils de détection" par la loi et n'enregistrent que des métadonnées, des données opérationnelles et de configuration à un point du réseau désigné. Les conditions d'exploitation sont déterminées par l'inspecteur de la cyberdéfense, nommé par le gouvernement de la République tchèque pour cinq ans à la fois. Les critiques soulignent le manque de contrôle (les soldats se contrôlent eux-mêmes), le risque de pratiques similaires au projet B*oundless Informant*, à XKEYSCORE, aux échanges entre la NSA et les services secrets britanniques GCHQ, *etc*. L'obligation de fournir des informations aux organes actifs dans le cadre d'une procédure pénale est régie par l'article 88a du code de procédure pénale (loi n° 141/1961).

En Slovaquie, l'obligation des opérateurs mobiles de conserver les données de connexion est définie dans la loi sur les communications électroniques n° 351/2011[25]. Selon cette législation, il n'y a pas de période de temps exacte définie dans cette loi. C'est aux opérateurs de téléphonie mobile de décider des détails de leur politique de stockage des données.

De son côté, le Portugal impose aux opérateurs de conserver les données de connexion pendant une durée d'un an (article 6 de la loi n°32/2008) alors que Chypre interdit toute conservation des données des clients par les fournisseurs de télécommunications : la conservation est illégale hors des cas très spécifiques dont le cadre légal a été fixé par les autorités. Il s'agit des enquêtes portant sur certains délits spécifiques et graves et uniquement après autorisation du procureur général ou du tribunal.

Enfin, en France la réglementation française impose aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus, la conservation généralisée et indifférenciée, pour une durée d'un an, des données de connexion de leurs utilisateurs (les données de trafic et de localisation des utilisateurs, leurs données d'identité civile, certaines données concernant leurs comptes et les paiements qu'ils effectuent en ligne). Le dispositif national s'aligne alors sur la jurisprudence de la Cour de justice de l'Union européenne[26], position reprise par la jurisprudence du Conseil d'État[27]. Ainsi, le droit français impose aux opérateurs de télécommunication de conserver les données de connexion de leurs utilisateurs à des fins de lutte contre la criminalité et le terrorisme. La conservation généralisée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, comme cela est requis par la CJUE. Conformément aux exigences de la Cour, il impose au Gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace[28].

[25] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/20140101.html.
Version ancienne du dispositif en vigueur jusqu'au 31/08/2014 (https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/20140101.html) : aux termes du paragraphe 58 article (5) : "Aux fins du paragraphe 7, l'entreprise est tenue de stocker les données relatives au trafic, les données de localisation et les données des parties communicantes à partir de la date de la communication pendant a) 6 mois pour la connexion à Internet, le courrier électronique par Internet et la téléphonie par Internet, et b) 12 mois pour les autres types de communication.".

[26] CJUE, 6 octobre 2020, Privacy International, aff. C-623/17 ; La Quadrature du Net e.a., French Data Network e.a., aff. C-511/18 et C-512/18 ; Ordre des barreaux francophones et germanophone e.a., aff. C-520/18.

[27] CE, arrêt du 21 avril 2021, N° 393099.

[28] https://www.conseil-etat.fr/actualites/actualites/donnees-de-connexion-le-conseil-d-etat-concilie-le-respect-du-droit-de-l-union-europeenne-et-l-efficacite-de-la-lutte-contre-le-terrorisme-et-la.

En revanche, il juge illégale l'obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins autres que ceux de la sécurité nationale, notamment la poursuite des infractions pénales.

En effet, par l'adoption de trois arrêts du 6 octobre 2020, la Cour de justice de l'Union européenne (CJUE) est venue interdire la conservation généralisée et indifférenciée des données de connexion par les opérateurs tout en posant plusieurs exceptions à cette interdiction, en précisant notamment les types de données qui peuvent faire l'objet d'une conservation à titre préventif. Il s'agit tout d'abord des données de trafic et de localisation lorsque la conservation est ciblée en fonction des catégories de personnes ou d'une zone géographique préétablie en raison du risque criminogène. Pour pouvoir procéder à une telle conservation, il faut que l'État membre soit « confronté à une menace grave pour la sécurité nationale, qui s'avère réelle et actuelle ou prévisible ». Plusieurs conditions doivent alors être remplies :

- La conservation des données de connexion doit faire l'objet d'une injonction par une autorité publique ;
- Cette injonction doit être soumise à un contrôle effectif d'une juridiction ou d'une autorité administrative indépendante ;
- L'injonction doit être limitée dans le temps, mais peut être renouvelable en cas de persistance de la menace.

La CJUE vise alors les données de connexion qui « sont susceptibles de contribuer à l'élucidation d'une infraction grave ou à la prévention de menaces graves contre la sécurité publique ».

Ensuite, la Cour de La Haye vise les adresses IP. S'agissant de ces informations, leur conservation généralisée et indifférenciée peut être autorisée « dès lors qu'elle peut constituer le seul moyen d'investigation permettant l'identification d'une personne ayant commis une infraction en ligne »[29].

Puis, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs est autorisée par la Cour lorsqu'il s'agit de prévenir des menaces liées à la sécurité publique. Elles sont utiles en vue de rechercher, de détecter et de poursuivre des infractions pénales définies par le législateur.

[29] https://itlaw.fr/donnees-de-connexion-quelles-sont-les-limites-a-leur-conservation/.

Enfin, dans le respect de la réglementation en vigueur en matière de protection des données à caractère personnel, la Cour européenne vient rappeler que tout mécanisme de conservation de données autorisée doit néanmoins présenter les garanties effectives contre les risques d'abus.

En conclusion, si la Cour de justice de l'Union européenne a fixé un cadre légal relatif à la conservation préventive des données de connexion, il n'en demeure pas moins une distorsion dans les dispositifs nationaux, particulièrement concernant la durée de conservation que l'autorité nationale peut imposer aux opérateurs. Il semble alors indispensable de procéder à une harmonisation de l'ensemble des obligations légales en la matière participant alors à l'effort de clarification et d'efficacité des politiques pénales visant à lutter contre les formes graves de criminalité transnationale.

Présentation de la checklist de l'enquêteur :

- La liste est divisée en 5 phases (de l'enquête). Il ne s'agit pas de suivre obligatoirement chaque phase de l'enquête.
- Il est possible, après chaque phase, d'ajouter des remarques à la check-list.
- La check-list se réfère aux articles de loi d'application. L'enquêteur est ainsi en mesure de se procurer des renseignements complémentaires.
- Pour certaines étapes, des formulaires standards peuvent être utilisés. S'ils sont disponibles, vous pourrez cliquer sur les liens dans la check-list pour ainsi ouvrir directement lesdits formulaires/documents.
- La check-list contient également des hyperliens vers des documents utiles sur l'étape à effectuer.

***NB** : les références textuelles inscrites dans le document sont issues des textes applicables en Belgique.*

Il s'agira de proposer le document de façon appropriée et comportant les références légales de chaque État membre.

À cet effet, un travail en collaboration avec les agents d'Europol, d'Eurojust et/ou les points contacts nationaux pourrait être bénéfique à la réussite du projet. Un travail collaboratif et efficace permettra aux enquêteurs et aux magistrats de disposer des sources textuelles

correctes et de voir leurs requêtes aboutir plus facilement, participant alors à l'efficience de la justice pénale et de la coopération européenne.

A l'issue de l'édification du document, des séances de « prise en main », de simulations, de mises en situation devront être organisées pour permettre à l'ensemble des acteurs concernés de maîtriser ce nouveau support de travail. Ces séances, indispensables, favoriseront une bonne exploitation de ce document ce qui participera à la réussite de l'enquête. Le CEIFAC, en qualité d'organisme de formation pourra assurer l'élaboration, la coordination et l'animation de tels ateliers de formation.

i. Prise de connaissance du délit

Nature des activités	*Renseignements supplémentaires*			*NA*	*PV*
Première vérification sommaire	• Patrimoine illégal à chiffrer ? • Éléments de patrimoine illégal présents ? • Utilisation des techniques OSINT* (evt. consultation via service I-2 Recherche Internet) *Techniques OSINT : vérification des entités dans les différents moteurs de recherche, vérification sur les médias sociaux, I2, …			☐ ☐ ☐	
Entités enquête patrimoniale	• Quelles entités entrent en ligne de compte pour une enquête financière ? * Peut être aussi bien une personne morale que physique. * Peut s'étendre à un tiers qui n'est pas impliqué dans le délit même (ex partenaire): délit de blanchiment			☐	

Remarques

ii. Premiers actes d'enquête

Nature des activités	*Renseignements complémentaires*			*N A*	*PV*
Concertation avec le magistrat (écrite/orale)	• Motivation de l'enquête "patrimoniale/ Équipe PLUK" à l'aide du plan d'enquête • Demande des apostilles nécessaires ○ Consultation dossier fiscal (TVA, imposition directe, ISI) ○ Consultation du cadastre, des hypothèques, enregistrements et domaines ○ Créances bancaires simples * ○ Créances bancaires élargies ○ Identification comptes bancaires ** Relevé de comptes (et solde) + coffres-forts* ** Les réquisitoires aux banques/cartes de paiement/ transferts d'argent/ sociétés boursières peuvent être faits au moyen de la même apostille (avec la fourniture des données nécessaires)*			☐ ☐ ☐ ☐ ☐ ☐	
Autres banques de données	• EuroDB / BCE • Registre UBO • Douane (sans réclamation) – import/export EG argent cash > 10.000 euro			☐ ☐ ☐	

	• Cartes de paiement (identification, comptes liés, dépenses, lieux dépenses– si recevable) • Compagnies d'assurance (assurance-vie, branche 21, branche 23, épargne pension) * • Bureaux de change • Transferts d'argent (envoi, réception d'argent cash) • Sociétés boursières (ex. Comptes de titres chez Binck Bank, Bolero, Lynx,…) • DIV/Bateaux/avions/héli • Jeux de hasard (casinos, loterie nationale) - CJH • Info étranger ** Lors de recherches au sein d'une compagnie d'assurance, contrôler si l'intéressé est **preneur d'assurance** ou **bénéficiaire**. Éventuellement vérifier si une tierce personne (ex. partenaire, membre de la famille, enfant,…) est bénéficiaire.*			☐ ☐ ☐ ☐ ☐ ☐ ☐	
Estimation du patrimoine illégal	• Déjà possible à ce stade de l'enquête ? ** Calcul sommaire (les premières indications sont suffisantes pour justifier une ordonnance de saisie (par équivalent).*			☐	
Analyses	• Analyse du dossier fiscal			☐	

	• Analyse des données cadastrales • Analyse des comptes			☐ ☐	
Déjà des soupçons de patrimoine à l'étranger ? *(ex. par analyse des comptes bancaires, consultations des vols, nationalité…) ** soupçon de transaction suspecte à l'étranger ou suspect de par la nationalité (ex. fonctionnaire de l'UE)* ** via par exemple la base de données PNR (Passenger Name Record)*	• Consultation pays via application SIENA (réseau ARO) • Ou via e-mail LO auprès de l'OCSC. * o But de la demande : • Biens immobiliers • Véhicules/bateaux/avions • Mandat en entreprise (ex. administrateur, gérant,…) ** Si demande via LO de l'OCSC (Office Central Saisie et Confiscation), les données suivantes doivent être communiquées :* • *Numéro de notice* • *Bref résumé des faits* • *Lien avec pays consulté*			☐ ☐ ☐ ☐ ☐	

iii. Activités préalables à une perquisition

Nature des activités	*Renseignements complémentaires*	*Oui*		*NA*	*PV*
Existe-t-il des indications de distorsions entre le dossier fiscal et le niveau de vie réel ? * Engagement chien renifleur de billets * Recherche sur la comparaison des actifs : article 43 quater du code pénal, Belgique * Blanchiment de capitaux : article 505 § 1, 2°, 3° et 4° CP	• tous les (co)auteurs au cours d'une période suspecte de 5 ans • tous les tiers en ce qui concerne le blanchiment de capitaux • Contact service appui canin	☐ ☐ ☐		☐ ☐ ☐	
Blocage comptes/coffres-forts * * Article 46 quater § 2 CIC (devoir de coopération des banques : article 46 quater § 3 CIC)	• Demande de blocage du compte par la banque • (comptes uniquement pour le débit) -> de cette façon, l'argent peut toujours être déposé sur le compte • Demande de blocage des coffres-forts	☐ ☐ ☐		☐ ☐ ☐	

Blocage patrimoine à l'étranger * *** *Ordonnance 2018/1805 du Parlement Européen et du Conseil de l'UE dd. 14 novembre 2018 (publiée dans le journal officiel de l'UE avec numéro L 303/1 dd. 28-11-2018)***	• *Certificat de gel + certificat de confiscation/instruction* -> signé par PdR/JI • *Certificat de gel transmis à OCSC* ? • Si perquisition à l'étranger -> CRI / DEE (Administrative ou avec déplacement) ** attention : pour analyse d'un compte bancaire -> via CRI (peut être subséquent à un freezing order/ Certificat de gel)*	☐ ☐ ☐		☐ ☐ ☐	
Saisie conservatoire biens immobiliers * Saisie des biens immobiliers : article 35 bis CIC	• Bien immobilier identifié (voir plus haut) • Signification par huissier de justice • Transcription exploit de saisie dans registre des hypothèques • Notification à OCSC (obligatoire)	☐ ☐ ☐ ☐		☐ ☐ ☐ ☐	

Remarques

iv. <u>Activités pendant une perquisition</u>

Nature des activités	***Renseignements supplémentaires***			***NA***	***PV***
Existe-t-il des indications de distorsions entre le dossier fiscal et le niveau de vie réel ? * Perquisition dans habitation/entreprise + saisies (2*) * Recherche sur la comparaison des actifs : article 43 quater du code pénal * Blanchiment de capitaux : article 505 § 1, 2°, 3° et 4° CP (2*) Saisie : article 35 CIC.	• tous les (co)auteurs au cours d'une période suspecte de 5 ans • tous les tiers en ce qui concerne le blanchiment de capitaux • saisie argent cash • Saisie véhicules -> service de remorquage (réquisition judiciaire) • Engagement FCCU/RCCU (crypto monnaie ?)			☐ ☐ ☐ ☐ ☐	

Coffre bancaire ** Saisie : article 35 CIC.* ** Bris de scellés : article 283 e.s. Cp.*	• Scellement coffre bancaire (attention : risque de bris de scellés par rapport à coffre-fort de valeur) • Perquisition dans coffre bancaire ? Saisie avantages patrimoniaux			☐ ☐	
Blocage patrimoine à l'étranger * ** Ordonnance 2018/1805 du Parlement Européen et du Conseil de l'UE dd. 14 novembre 2018 (publiée dans le journal officiel de l'UE avec numéro L 303/1 dd. 28-11-2018)*	• *Certificat de gel + certificat de confiscation/instruction* -> signé par PdR/JI • *Certificat de gel transmis à OCSC* ? • Si perquisition à l'étranger -> CRI / DEE (Administrative ou avec déplacement) ** attention: pour analyse d'un compte bancaire -> via CRI (peut être subséquent à un freezing order/ Certificat de gel)*			☐ ☐ ☐	

Remarques

v. Activités directement après la perquisition

Nature des activités	*Renseignements complémentaires*			*N A*	*PV*
Existe-t-il des indications de distorsions entre le dossier fiscal et le niveau de vie réel ? * Analyse des éléments trouvés **** Recherche sur la comparaison des actifs : article 43 quater du code pénal*** **** Blanchiment de capitaux : article 505 § 1, 2°, 3° et 4° CP***	• tous les (co)auteurs au cours d'une période suspecte de 5 ans • tous les tiers en ce qui concerne le blanchiment de capitaux • Avantages supplémentaires probables intérieur/étranger • Calcul des avoirs illégaux possible ?			☐ ☐ ☐ ☐	
Audition* ** Il est préférable de mener un interrogatoire séparé*	• Confrontation suspect avec avantages illégaux			☐	

(car la demande de provenance des moyens peut porter sur des faits) -> donc pas en même temps que l'audition technique perquisition. (règles Salduz)					
Blocage patrimoine à l'étranger * * *Ordonnance 2018/1805 du Parlement Européen et du Conseil de l'UE dd. 14 novembre 2018 (publiée dans le journal officiel de l'UE avec numéro L 303/1 dd. 28-11-2018)*	• En Belgique ? • À l'étranger ? *Certificat de gel + certificat de confiscation/instruction* -> signé par PdR/JI • *Certificat de gel transmis à OCSC* ?			☐ ☐ ☐ ☐	
Soldes comptes bancaires bloqués * * *blocage temporaire compte bancaire : Article 46 quater § 2 CP vaut pour max 5 jours donc saisie à temps*)	• Saisie sur compte ○ Procédure par police ? ○ Procédure par magistrat ? • OCSC informé de la saisie sur compte (= notification) • Transfert de soldes de comptes bancaires bloqués vers le compte OCSC ? (pas d'état jaune nécessaire ici)			☐ ☐ ☐	

** saisie sur compte : Article 37 CIC*	** attention : article 37 CIC : en principe saisie sur compte -> transfert compte vers compte bancaire OCSC uniquement moyennant ordre magistrat responsable*				
Versement d'argent	• Argent cash sur compte OCSC (compte) • Notifier avec état jaune à l'OCSC			☐ ☐	

Remarques

Nature des activités	***Renseignements complémentaires***	***Oui***	***Non***	***NA***	***PV***
Analyse des éléments trouvés	• Avantages supplémentaires probables intérieur/étranger • Calcul des avoirs illégaux possible ?	☐ ☐	☐ ☐	☐ ☐	

Audition* ** Il est préférable de mener un interrogatoire séparé (car la demande de provenance des moyens peut porter sur des faits) -> donc pas en même temps que l'audition technique perquisition. (règles Salduz!!!)*	• Confrontation suspect avec avantages illégaux	☐	☐	☐	
Saisies supplémentaires nécessaires ?	• Intérieur ? • Étranger ? • Certificat de gel + certificat de confiscation/instruction -> signé par PdR/JI *Certificat de gel transmis à OCSC* ?	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐	
Notifications à l'OCSC	• Contrôler si toutes les saisies ont été notifiées à l'OSCS	☐	☐	☐	

Traitement et suivi dans GES (Application gestion d'Enquête)	• Input de toutes les saisies d'avantages patrimoniaux ○ Argent cash ○ Saisie sur comptes ○ Biens immobiliers ○ Saisies à l'étranger	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	

Remarques

vi. <u>Fin enquête</u>

Nature des activités	*Renseignements complémentaires*			*N A*	*PV*
Synthèse	• Résultats financiers enquête dans un procès-verbal (synthèse par entité) * • *Reprendre toutes les informations utiles dans ce procès-verbal. Pas seulement ce que l'intéressé a p ex reçu en pots-de-vin mais aussi ce qu'il ne dépense plus (dépenses manquantes)*		☐ ☐	☐ ☐	
Enquête patrimoniale particulière * * enquête patrimoniale particulière : article 524 bis CIC.	• Application de l'enquête patrimoniale particulière ?* * *Le suspect est déjà condamné pour un crime de base et l'enquête financière est scindée. Le procureur a 2 ans pour terminer l'enquête financière. Seulement si le parquet le réclame devant le juge en 1ère instance.*		☐	☐	
Enquête pénale d'exécution ? * * EPE : article 464/29 à article 464/40 CIC.	• Application de l'enquête pénale d'exécution ?		☐	☐	

7. La charte des victimes de cyberattaque

Un dernier acteur de la scène pénale reste à identifier : la cybervictime.

Bien que ce type de délit soit virtuel, la victime et les conséquences pour elle sont tout à fait réelles. Parmi les difficultés relatives à la prise en charge et l'accompagnement des cybervictimes, ont été relevées notamment :

- Le défaut de cartographie des cybervictimes car les statistiques ne montrent que la partie émergée de l'iceberg ;
- La mésestimation de l'impact d'une cyberattaque : le caractère virtuel de la cybercriminalité laisse à penser aux malfaiteurs et à la société que les effets de tels actes sont moins graves que ceux d'une infraction commise sur le plan physique ;
- La détermination du préjudice matériel, moral et réputationnel. Le préjudice d'une cyberattaque est difficile à mesurer et à prouver. Par conséquent, la réparation du dommage causé est souvent ressentie comme insuffisante pour et par les victimes. Il serait alors intéressant de se questionner sur l'opportunité de fixer des montants estimatifs tenant compte de paramètres objectifs, en suivant le modèle relatif au Fonds de Garantie des Victimes des actes de terrorisme et d'autres infractions (FGTI) qui est l'organisme chargé d'indemniser en cas d'infraction au titre de la solidarité nationale, à laquelle chaque assuré contribue. Il se retourne contre les auteurs des dommages afin d'obtenir le remboursement des sommes versées aux personnes victimes. Le système d'indemnisation des victimes d'infractions est actionné lorsque quelqu'un est personnellement victime d'une infraction pénale (homicides, viols et agressions sexuelles, violences conjugales, …), représente légalement une victime d'infraction pénale (mineur ou majeur protégé) ou est l'un des proches (conjoint, ascendant, descendant) décédé des suites d'une infraction pénale. Selon le principe de fonctionnement, sont exclus du traitement de la CIVI les dommages résultant d'infractions qualifiées d'actes de terrorisme (FGTI), d'accidents de la circulation survenus sur le territoire français (FGAO), d'actes de chasse (FGAO), des maladies liées à l'amiante (FIVA), infractions pour lesquelles des fonds spéciaux ont été mis en place. Suivant ce modèle, il serait envisageable de mettre en place à l'échelle européenne un fonds dédié à l'indemnisation des victimes de cyberattaques, fonds dans lequel pourrait puiser chaque entité juridique nationale et pour laquelle chaque État contribuerait au nom de la solidarité entre citoyens européens. Il faudra alors fixer des critères objectifs permettant d'actionner le paiement d'indemnités à la victime, à savoir : le temps d'arrêt de fonctionnement d'une entreprise attaquée, la gravité dans le dysfonctionnement du système, la perte de productivité, les coûts immatériels (réputation de l'organisme, confiance des clients et des partenaires, …), le recours à un prestataire spécialisé pour contrer ou résoudre les dommages résultant de la cyberattaque, les coûts de récupération des données, le nombre d'heures d'assistance pour résoudre les problèmes, les pertes d'opportunités commerciales et financières, la souffrance morale et les préjudices extra patrimoniaux, …. Cette grille permettrait par la même occasion d'aider les

victimes, avocats, organismes payeurs, assurances, ou encore les magistrats à mieux se positionner au moment de la reconnaissance du statut de victime de cyberinfractions.

- La capacité de préserver la preuve attestant le dommage enduré. Dans la plupart des messages visant à sensibiliser le public, il est demandé à l'usager de conserver la preuve de l'attaque. Or, la victime qui a subi la cyberattaque n'est pas forcément au fait des techniques relatives à la conservation et à la préservation des éléments qui pourraient servir de preuve à l'occasion d'une procédure pénale ;
- La considération tenant au coût du procès. Les faits commis sur Internet entraînent fréquemment l'ouverture d'investigations transnationales. Pour des victimes de cyberattaques, la prise en compte de ce facteur et les coûts pouvant s'y attacher peuvent effrayer. En effet, il faudra prendre en considération des aspects tels que les frais de conservation de la preuve numérique, les frais de déplacement pour témoigner, la faible indemnisation envisagée. Certes des cyberassurances existent mais elles sont encore à l'état embryonnaire[30]. Notons à ce sujet que face à l'explosion des cyberattaques et particulièrement des rançongiciels en France, un rapport parlementaire propose une série de mesures pour mieux structurer le marché de la couverture du risque cyber et mieux prévenir les risques. Il propose notamment une interdiction du paiement des cyber-rançons, une harmonisation des critères de risques ou la formation des agents généraux à ce risque[31]. L'enjeu est bien de renforcer l'écosystème numérique français en plein essor et, a fortiori, l'économie numérique européenne qui pourrait bénéficier d'une telle protection à l'échelle de l'Union ;
- Au moment du dépôt de plainte. Il est en l'espèce intéressant de se questionner sur la formation consacrée aux personnes responsables de l'accueil des cybervictimes. Il s'agit ici de s'assurer que les acteurs disposent des bonnes postures tant sur les aspects de procédure que ceux touchant à la psychologie des victimes. Il s'agit ici de s'assurer que les professionnels de la justice présentent ce que l'on peut qualifier de bonnes pratiques. En l'espèce, l'exemple de la Belgique pourrait servir de modèle pour l'édification d'un cadre formatif des enquêteurs en charge du traitement des affaires touchant à la cybercriminalité. En effet, la Direction DGJ-DJSOC de la police belge a lancé début octobre 2020 le projet « *Hub Sharepoint Cyberaid* », opérationnel à l'été 2021. Ce nouveau dispositif présente trois objectifs que sont : l'aide aux policiers de première ligne lorsqu'il recueille une plainte et conseille les victimes lors du dépôt de plainte ; l'appui aux enquêteurs pour les devoirs à effectuer après le recueil de la plainte et enfin, le document recèle un ensemble d'informations générales en lien avec les bonnes pratiques à adopter ou encore les offres de formation disponibles en la matière. Figurent au projet, un

[30] En 2020, le volume de primes a augmenté de 49% (à 130 millions d'euros), le montant des indemnisations versées a, lui, été multiplié par 3 (à 217 millions d'euros en 2020), soit un ratio combiné qui est passé de 84 % en 2019 à 167 % en 2020. Pour la même période, l'*Anssi* a enregistré une augmentation de 225% des signalements d'attaques par rançongiciels par rapport à 2019, https://www.ssi.gouv.fr/agence/missions/rapport-dactivite-2020/

[31] https://www.lassuranceenmouvement.com/wp-content/uploads/2021/10/Rapport_La-Cyber-assurance_Valeria_Faure-Muntian_13102021.pdf.

certain nombre de principes qui pourraient être transposables à l'Union européenne tels que l'accès à la plateforme dans l'ensemble des langues nationales belges (français, néerlandais et allemand), aspect linguistique qui a toute son importance dans un espace multiple.

Il semble indispensable que les enquêteurs en charge de l'accueil des cybervictimes puissent disposer de formations qui peuvent être construites suivant le modèle des formations proposées lorsqu'il s'agit d'entendre des mineurs victimes d'infractions à caractère sexuel ou de personnes victimes de violences intrafamiliales. En France, par exemple, la police propose deux formations dénommées « formation ICC » (investigateur en cybercriminalité[32]) et « formation PIC » (primo intervenant en cybercriminalité). Ces deux formations internes au corps des policiers français présentent la caractéristique d'être très technique. De plus, depuis 2018 plusieurs formations internes sur cette thématique sont proposées sous la forme d'un enseignement dispensé en e-learning pour un volume horaire de huit heures au cours desquelles l'enquêteur se forme aux bases de l'investigation numérique, se familiarise avec le Darknet et se forme à la typologie des actes de cybercriminalité. En revanche, il ressort un manque de formation initiale pour les gardiens de la paix qui sont en première ligne et sont les premiers interlocuteurs de la victime lorsque cette dernière désire porter plainte. Au vu de l'augmentation importante des actes de cybermalveillance, une meilleure prise en charge et un accueil adapté des victimes pourraient être alors enseignés pendant une dizaine d'heures lors de la formation initiale des policiers, formation qui pourrait être renouvelée lors des formation externes et internes, initiales ou continues des officiers de police judiciaire.

La gendarmerie française a également mis en place une formation spécialisée à destination des enquêteurs en matière d'accueil et de prise en charge des victimes de cyberattaques. Pour assurer un accueil respectueux des victimes, un système de « référents cyber ». Ce gendarme spécialement formé à la question va suivre le dossier ou venir en soutien de l'enquêteur en charge du dossier. La gendarmerie dispose également d'un protocole qui indique la posture d'accueil à adopter, les questions à poser à la victime, le nom des référents techniques et le moment opportun pour faire appel à l'officier spécialisé dans les nouvelles technologies.

- Le chiffre noir. Tous les facteurs cités en amont contribuent à accentuer ce phénomène, renforcé par d'autres éléments tels que le délai de détection des attaques car certaines victimes ne sont pas conscientes que le fait commis constitue une infraction pénale, pour d'autres, le préjudicie est jugé trop faible pour porter plainte et donner de la visibilité à l'infraction.

[32] https://www.francecompetences.fr/recherche/rncp/32061/ : qualification de niveau 6, cette formation a pour but de mener l'investigateur en cybercriminalité de sécurité intérieure à conduire les investigations techniques nécessaires à la matérialisation d'infractions dans le domaine des technologies de l'information et de la communication. Il assure une expertise dans le domaine des infractions liées aux technologies de l'information et de la communication et constitue un point privilégié d'interface avec les laboratoires d'investigations opérationnelles du numérique. Il assure également l'évolution du métier dans le domaine de la cybercriminalité.

- L'accessibilité au réseau associatif. Il est intéressant de constater que le grand public a connaissance des possibilités de s'adresser à des services gratuits et confidentiels lorsqu'il en ressent le besoin. Il serait dès lors opportun de dresser une liste actualisée et actualisable des associations d'aide aux cybervictimes de l'UE, liste facilement accessible, en différentes langues et identifiant les points de contact et les capacités de chacune (assistance technique, financière, juridique, …).

- Les dispositifs de signalement. Actuellement un grand nombre de sites et de plateformes de signalement se côtoient. Cet état de fait peut donner lieu à des confusions et à une perte de l'information utile pour le bénéficiaire. Il est intéressant de se questionner sur le mode de signalement le plus adapté ; de voir si la répétition des signalements est opportune ; et enfin, d'étudier la connaissance du consommateur quant à la différence entre un signalement et un dépôt de plainte.

- La langue. L'initiative du centre de lutte contre la cybercriminalité européen concernant la sensibilisation du public est très positive, mais force est de constater que tous les textes ne sont pas traduits. Les personnes qui ne maîtrisent pas (ou peu) l'anglais sont alors lésées dans leur accompagnement.

Recommandations

1. Analyser les avantages et les inconvénients du dépôt de plainte.
2. La formation spécialisée des responsables de la prise en charge des victimes de cyberinfractions est indispensable.
3. L'adoption d'une charte européenne des droits des cybervictimes semble le bon point de départ pour une réglementation harmonisée sur le territoire européen en la matière.
4. L'ensemble de ces préconisations a pour objectif de contribuer à renforcer les prérogatives de celles et ceux qui ont subi une cyberattaque et à réduire les risques d'une re-victimisation. A ces fins, il semble utile de s'inspirer des textes tels que le guide des droits de la victime diffusé par le ministère de la Justice française et le guide des Droits de l'Homme pour les utilisateurs d'Internet, publié par le Conseil de l'Europe[33]. Ce texte affirme d'ailleurs que « les États signataires de la Convention de Budapest se sont engagés à protéger les citoyens des activités criminelles et des infractions pénales commises sur Internet. Les utilisateurs d'Internet attendent raisonnablement d'être protégés contre les activités criminelles et les infractions pénales commises sur l'Internet ou par

[33] https://www.coe.int/fr/web/freedom-expression/guide-to-human-rights-for-internet-users : Le Guide des droits de l'homme pour les utilisateurs d'internet a été rédigé afin de présenter de manière conviviale les droits et les libertés garantis aux internautes par la Convention européenne des droits de l'homme. Ce guide a été pensé comme un outil de formation des citoyens à leurs droits lorsqu'ils naviguent sur internet et comme une incitation envers les gouvernements, les organismes publics et les entreprises à assumer leurs responsabilités quant à la protection adéquate des droits de l'homme en ligne.

l'utilisation d'Internet ». Les cybervictimes méritent de comprendre et d'exercer leurs droits qui ont la même valeur que l'on se situe dans le monde réel ou dans le monde virtuel. La charte devrait alors être disponible à l'accueil des commissariats et des brigades de gendarmerie, sur les plateformes de dépôt de plainte en ligne et sur tous les sites officiels des autorités compétentes. Ce document devra contenir les droits, libertés et garanties en lien avec :
l'accès à la justice (par exemple : quels dispositifs de prise en charge financière sont envisageables).
l'autorité compétente pour recueillir la plainte.
l'accès aux informations et la liberté d'information.
l'affirmation d'un accueil, d'une écoute attentive et respectueuse.
l'interaction avec des professionnels formés à la matière (ce qui garantira la qualité de l'accueil).
la protection de la vie privée et des données personnelles.
la transparence dans les démarches et les formalités relatives à la recevabilité de la plainte.
l'explication claire et la différenciation entre le dépôt de plainte et le signalement.
les délais pour déposer plainte.
les informations relatives à la procédure après le dépôt de la plainte.
les conditions et les formalités pour demander réparation et le remboursement des frais de justice.
le parcours de l'enquête.
l'information sur le droit à l'accompagnement pendant toutes les phases importantes de la procédure (y compris en cas d'investigation transfrontalière).
les voies de recours à chaque étape de la procédure.
les obligations des associations d'aides aux victimes (droits et limites à l'exercice d'une action).
les obligations des fournisseurs de service Internet.
l'obligation des pouvoirs publics dans la protection des citoyens contre les infractions commises en ligne. Dans cette rubrique, un résumé des textes légaux devrait être disponible. Il serait également intéressant de proposer des infographies et différentes ressources destinées à porter à la connaissance des victimes l'ensemble des éléments indispensables lui permettant de prendre une décision éclairée[34].

5. La charte des droits des cybervictimes pourrait enfin être accompagnée d'un guide et ses annexes adapté à chaque État membre qui recèlerait les textes et réglementations applicables au niveau national, la liste des contacts utiles et un lexique des termes.
6. Enfin, un partenariat avec *Victim Support* Europe pourrait être utile à la confection d'une telle charte à visée globalisée et humaine.

[34] En suivant par exemple, le système canadien : *https://www.justice.gc.ca/fra/sjc-csj/dlc-rfc/ccdl-ccrf/ in https://www.justice.gc.ca/fra/sjc-csj/dlc-rfc/ccdl-ccrf/ressources-resources.html.*