LA CRISE SANITAIRE MONDIALE, UN CONTEXTE FAVORABLE À LA CYBERCRIMINALITÉ

PAR **Vincent LE TROUHER,**

CHARGÉ DE MISSION LUTTE CONTRE LA FRAUDE, ENTREPRENEUR,
AUTEUR DE « DROIT PÉNAL DES AFFAIRES ET GROUPES DE SOCIÉTÉS. UNE SOUPLESSE PROPICE AUX INFRACTIONS ET À L'IMPUNITÉ » (L'HARMATTAN)

JANVIER 2022

OBSERVATOIRE DES CRIMINALITÉS INTERNATIONALES

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

En février 2021, le cabinet d'expertise-comptable CDER a été victime d'une escroquerie relevant de la « fraude au président » de presque 15 millions d'euros[1]. Il s'agit du plus gros préjudice financier jamais enregistré sur le territoire français pour des faits de la sorte. Ce type de criminalité s'est considérablement accru du fait de la digitalisation des rapports économiques et plus récemment du contexte de la crise sanitaire liée au Covid-19. Cette délinquance astucieuse érige la cybercriminalité en une menace prépondérante. Aux États-Unis, en avril 2021, le patron de la FED, la banque centrale américaine, en a fait un risque majeur pour l'économie et s'est déclaré « plus inquiet du risque d'une cyberattaque à grande échelle que d'une crise financière semblable à celle de 2008 ».

DE QUOI PARLE-T-ON ?

La « fraude au président » est une escroquerie[2] relevant de la catégorie des faux ordres de virement international (FOVI). Concrètement, elle « fait intervenir un imposteur se faisant passer pour le dirigeant d'une société qui exige d'un employé du véritable dirigeant de l'entreprise un versement rapide et confidentiel d'une somme d'argent sur un compte à l'étranger »[3]. Plus précisément, le fraudeur peut se présenter comme le président de la société ou comme son avocat et va ainsi : « contacter sa cible par téléphone et/ou mails et mettre en place tout un système de communication reposant sur le recours à de fausses adresses de messageries présentant de grandes similitudes avec les adresses concernées »[4]. Afin de parvenir à ses fins, le fraudeur va utiliser les failles identifiées préalablement de l'entreprise ciblée en les utilisant à son avantage par une ingénierie sociale très sophistiquée. Dès lors, le fraudeur s'infiltre dans les interstices de l'entreprise et découvre des informations confidentielles et utiles à son forfait. Il est alors en capacité d'utiliser des informations, comme un déplacement ou un congé prévu par le président de

[1] Matthieu MERCIER – « Arnaque au faux président : l'entreprise CDER de Châlons-en-Champagne escroquée de 15 millions d'euros ». Février 2021 ; publié sur le site de *France 3 Grand Est*.

[2] L'article 313-1 du Code pénal dispose que : « L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service un service ou à consentir un acte opérant obligation ou décharge ».

[3] Jean-Louis DI GIOVANNI et Éric LENOIR – « Autonomie d'une arnaque au président » ; publié sur le site *Silicon.fr* (site spécialisé dans l'actualité des technologies de l'information).

[4] Jean-Louis DI GIOVANNI – « Attention, la fraude au président est de retour ! » ; publié sur le site de *PwC*.

la société, pour mieux les mobiliser contre l'entreprise victime en se faisant passer pour lui. Il cherchera aussi le moment opportun pour être confronté à un adjoint, sachant que le responsable financier est en congés. Il pourra ainsi prétexter « la signature urgente d'un contrat stratégique – à partir duquel – l'usurpateur demande d'effectuer rapidement le virement bancaire »[5].

Dans un contexte où les attaques se multiplient, la « fraude au président » fait toujours recette étant entendu qu'elle ne nécessite pas une grande technicité dans sa forme la moins sophistiquée, restant ainsi accessible aux nombreux petits escrocs disséminés dans le monde entier. En revanche, certains criminels ont su complexifier sa mise en œuvre, la rendant redoutable car extrêmement difficile à déceler, y compris pour les cabinets de conseil censés lutter contre cette menace. Il est notamment intéressant de rappeler que les plus gros préjudices financiers résultant de cette fraude ont été recensés dans des cabinets d'expertise-comptable. Le dernier record en date pour une attaque similaire était détenu par un autre cabinet d'expertise-comptable, parmi les plus courus de la place, KPMG, célèbre cabinet du *big four* mondial, avait en effet été victime d'une fraude en 2012 pour un montant alors estimé à plus de 7 millions d'euros. Si la fraude prend les traits d'une « fraude au président » et résulte d'une particulière sophistication, elle « engage aussi une chaîne de responsabilités, qui interroge le contrôle interne d'un groupe lui-même chargé de la mettre en œuvre chez ses clients »[6].

MODUS OPERANDI

Traditionnellement, la tromperie consubstantielle à l'escroquerie et usitée dans le cadre de la « fraude au président » se fait par l'usage d'un faux nom et/ou d'une fausse qualité selon les dispositions de l'article 313-1 du Code pénal[7]. C'est pourquoi on évoque l'usurpation d'identité. Cependant, la « fraude au président » n'a cessé de se complexifier, grâce, notamment, au développement du numérique. Dans un contexte où la crise du Covid-19 a joué un rôle favorable, eu égard à la dématérialisation des interactions favorisée par le télétravail, la cybercriminalité s'est imposée comme une menace prédominante. Il va sans dire que : « le travail à distance a banalisé les échanges par téléphone et a donc augmenté les risques de fraudes de ce type ». À ce titre et depuis le début de crise sanitaire, on ne compte plus les semaines sans que l'actualité ne fasse

[5] Éric VERNIER et Vincent LE TROUHER – « Fraude au président : la crise sanitaire a déclenché une nouvelle vague d'attaques », Janvier 2021 ; publié sur le site *The Conversation* et relayé par *La Tribune*.

[6] Denis LAFAY – « KPMG : Les dessous d'une escroquerie de 7,6 millions d'euros ». Juin 2014 ; publié sur le site de *La Tribune Auvergne-Rhône-Alpes*.

[7] Le procédé de tromperie le plus usité dans le cadre de l'escroquerie est le faux nom ou la fausse qualité.

mention de la paralysie d'un hôpital du fait de cyberattaques[8]. Ainsi, en 2021, nombre d'hôpitaux comme ceux de Narbonne, Montpellier, Dax, Villefranche-sur-Saône ont été attaqués par des rançongiciels. Le rançongiciel ou *ransomware* en anglais est : « un programme installé par les attaquants sur le réseau qui chiffre les données, exigeant dans le même temps une rançon, généralement en bitcoin, pour obtenir une clé de déchiffrement »[9]. Personne n'est épargné car ce procédé se développe aussi auprès des mairies. On peut dans ce registre citer la paralysie dont a été victime la mairie d'Angers à la suite d'un rançongiciel les 15 et 16 janvier 2021[10].

La cybercriminalité a ouvert une nouvelle ère, sur fond de professionnalisation des fraudeurs, complexifiant de facto les attaques et favorisant leur croissance. Cette capacité d'adaptation se caractérise surtout par : « l'hybridation de ses procédés de tromperie que l'on retrouve aisément au sein des manœuvres frauduleuses, élément matériel de l'escroquerie »[11].

Les confinements successifs liés au Covid-19 entre 2020 et 2021 ont accéléré la dématérialisation des échanges (mail, téléphone, réunion à distance…) apparue il y a une vingtaine d'années. Elle est désormais appréhendée comme une solution pérenne indispensable pour maintenir l'activité économique. Le transfert des interactions « présentielles » vers les interactions « distancielles » a corrélativement permis aux fraudes numériques de prospérer grâce à des fraudeurs proposant des stratagèmes de plus en plus complexes pour gagner en efficacité. En outre, le contexte anxiogène du confinement a altéré le respect des règles d'usage élémentaires en la matière malgré des appels à la prudence. Dans ce contexte, la commissaire divisionnaire Anne-Sophie Coulbois, cheffe de l'Office central pour la répression de la grande fraude financière (OCRGDF), indiquait à France Bleu[12] que la meilleure marche à suivre était de ne pas céder à la panique et à l'urgence des injonctions faites par les fraudeurs.

---

[8] Nicolas RAULINE – « La cybercriminalité, principal risque pour l'économie, selon Jérôme Powell ». Avril 2021 ; publié sur *Les Echos*.

[9] Louis ADAM – « Hôpitaux et ransomwares : Les cybercriminels savent très bien où ils sont ». Mars 2021 ; publié sur le site spécialisé *ZD Net*.

[10] Victoria GEFFARD – « Angers. Ce que l'on sait de la cyberattaque qui frappe les sites de la mairie ». Janvier 2021 ; publié sur le site de *Ouest-France*.

[11] Vincent LE TROUHER – « La fraude au président à l'ère de la Covid-19 ». Novembre 2020 ; publié sur LinkedIn et *Village de la Justice* – Op.cit.

[12] Martine BRESON – « Coronavirus – Des escrocs profitent de la crise pour arnaquer les hôpitaux, les pharmacies et les EHPAD ». Avril 2020 ; publié sur *France Bleu*.

DES GAINS IMPORTANTS

Même si les fraudeurs sont des professionnels aguerris et plus particulièrement « des groupes criminels organisés extrêmement spécialisés et rodés » précise Anne-Sophie Coulbois[13], il convient d'observer que la multiplication de ces fraudes résulte des gains substantiels susceptibles d'être engendrés. À ce titre, l'universitaire Éric Vernier observe « qu'on assiste au pillage de réserves sanitaires, à des arnaques en tout genre sur internet, à la vente de contrefaçons de produits sanitaires ou de médicaments, à l'explosion des cyberattaques pour pirater les données »[14]. En témoigne l'exemple d'une entreprise rouennaise, lestée de 6,5 millions d'euros lors d'une commande de masques et de gel hydroalcoolique à une entreprise fantôme[15]. Un phénomène qui touche un nombre croissant de pays à travers la planète et qui a conduit le Bureau Canadien du Crédit a forger le terme de « corona-fraude »[16]. L'internationalisation de la « fraude au président » a favorisé sa propagation par l'intermédiaire de la cybercriminalité. À ce titre, les coûts liés à la cybercriminalité ont explosé et n'ont cessé d'augmenter dans le monde. En cinq ans, ils ont plus que doublé, dépassant désormais les 1 000 milliards de dollars par an[17]. Plus précisément, les vols de données et les dommages engendrés par les virus informatiques représenteraient 1 % du PIB mondial d'après une étude de McAfee et du Centre d'études stratégiques et internationales (CIS)[18].

Comme pour de nombreuses autres escroqueries en ligne, la dimension internationale de la « fraude au président » se caractérise également par le versement du produit de la fraude par l'entremise de virements internationaux. Plus spécifiquement, il apparaît que ceux-ci sont effectués vers des territoires ne pratiquant que peu ou pas d'extraditions et où les fraudeurs ont élu domicile, en Asie notamment. Cette dimension internationale, outre la sophistication des procédés, rend plus complexes et plus longues les investigations judiciaires, qui requièrent une expertise éprouvée de la part des enquêteurs.

[13] Dépêche AFP – « Coronavirus : les arnaques se multiplient ». Avril 2020 ; publiée sur *France Info*.

[14] Éric VERNIER – « La chloroquine sera vendue par des criminels ». Mars 2020 ; publié sur le site de l'IRIS.

[15] Delphine GOTCHAUX – « Coronavirus : attention au retour de « l'arnaque au président », ou « aux faux ordres de virement » ». Avril 2020 ; publié sur le site *France Info* – Op.cit.

[16] Bureau Canadien du Crédit – « Une pandémie de fraude à venir, la Corona-fraude ! ». Mars 2020 ; publié sur le site du Bureau Canadien du Crédit.

[17] Florian DEBES – « Cybercriminalité : la facture ne cesse de s'alourdir ». Décembre 2020 ; publié dans *Les Echos Entrepreneurs*.

[18] Florian DEBES – op.cit., décembre 2020.

RENFORCER LA COOPÉRATION INTERNATIONALE

Cette menace globalisée exige aussi le renforcement de la coopération pénale internationale. À cet égard, l'entrée en vigueur et l'effectivité du Parquet européen seraient peut-être une solution, à l'échelle européenne, pour mieux combattre la prolifération de la « fraude au président ». Europol, l'agence européenne de police criminelle, a, pour sa part, apporté des réponses efficaces et pertinentes face à la criminalité évoluant dans le cyberespace. La vocation très opérationnelle de la section EC3 a permis de faire des liens dans des enquêtes internationales complexes et de gagner en efficacité, notamment par un partage plus rapide des informations via Europol sans pour autant faire préalablement une demande pénale d'entraide internationale. De la même manière, le phénomène du gel des données inscrit au sein de la Convention de Budapest[19] permet lui aussi une efficacité non négligeable. La capacité de figer une situation en attendant que le temps judiciaire fasse son office est un avantage incommensurable pour l'efficacité de l'enquête et sa résolution. Cette coopération pénale européenne a récemment porté ses fruits comme l'illustre le démantèlement d'un groupe de cybercriminels « soupçonné d'être à l'origine de plusieurs centaines d'attaques à travers des rançongiciels depuis septembre 2020 »[20]. Une vaste opération Franco-Ukrainienne a permis en effet d'interpeller plusieurs hackers suspectés d'être en rapport avec Egregor, attaque cybercriminelle de grande ampleur. Davantage pragmatique, la lutte contre la cybercriminalité se concentre sur l'annihilation immédiate du danger et de la menace.

À l'image des parquets nationaux financiers ou antiterroristes, un parquet spécialisé pourrait permettre non seulement d'absorber l'accroissement du contentieux, lequel menace d'engorgement la section J3 du Parquet de Paris[21], mais également d'offrir une réponse judiciaire satisfaisante dans un contexte où, en 2020, selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[22], les cyberattaques par rançongiciels ont augmenté de 255 %. Une augmentation substantielle qui laisse présager des attaques endémiques portant la menace cyber à un degré supérieur. Pour faire face à ce phénomène d'ampleur grandissante, un groupe parlementaire réuni en Commission Supérieure du Numérique et des Postes (CSNP) a donc proposé à l'exécutif 27

[19] La Convention de Budapest est une convention sur la cybercriminalité, premier traité international abordant la criminalité sévissant sur dans le cyberespace. Elle a été signée en novembre 2001 et est entrée en vigueur le 1er juillet 2004.

[20] Emmanuel LECLERE – « Cybersécurité : des pirates « Egregor », à l'origine de l'attaque contre *Ouest-France* interpellés en Ukraine ». Février 2021 ; publié sur le site de *France Inter*.

[21] La section J3 du parquet de Paris est la section spécialisée en cybercriminalité de la juridiction nationale chargée de la lutte contre la criminalité organisée.

[22] L'ANSSI est dirigée par Guillaume POUPARD.

recommandations pour lutter contre la cybercriminalité en France, dont la création d'un parquet national spécialisé dans la cybercriminalité. Même si le Parquet de Paris a créé en son sein une section J3 spécialisée dans la cybercriminalité, force est de constater que les moyens, notamment humains, alloués à cette section ne sont pas suffisants. Comme le constate le rapport de la CSNP : « seulement trois magistrats traitent les dossiers de cybercriminalité en France alors que le nombre d'attaques augmente à un rythme exponentiel depuis deux ans »[23]. Le dénuement et la paupérisation de la justice sont malheureusement des obstacles à l'efficacité de toutes actions contentieuses et des réponses judiciaires à donner face à la virulence de la menace. À ce propos, la grève inédite et historique du 15 décembre 2021 de la grande majorité des magistrats français en est une illustration dommageable.

UNE OPPORTUNITÉ À SAISIR

Si la Commission observe « une véritable carence » de l'État français en matière de moyens consacrés à la lutte contre la fraude, les parlementaires espèrent que la présidence du Conseil de l'Union européenne par la France au premier semestre 2022 pourra faire émerger la question de la cybercriminalité comme une véritable priorité. Il ressort du rapport de la Commission que « les parlementaires désirent que la France inscrive la sécurité et la protection de l'espace numérique européen au rang des priorités, et que « l'Europe doit trouver des voies et moyens de son autonomie afin de maîtriser ses dépendances à des technologies et des opérateurs extraeuropéens »[24]. Face à une menace grandissante, il est clair que l'Europe et a fortiori la France doivent bâtir une véritable souveraineté numérique pour éviter toute dépendance envers les États-Unis en premier lieu et la Chine dans un futur proche.

Malgré une nette, mais insuffisante, amélioration de la réponse publique européenne et française, la dimension mondiale du phénomène constitue une sérieuse limite à l'efficacité des outils dont les États disposent pour se prémunir de ces nouvelles menaces qui touchent certes les intérêts privés mais aussi ceux des nations.■

[23] Valentin CIMINO – « Le Parlement pousse pour la création d'un parquet dédié à la cybercriminalité ». Mai 2021 ; publié sur le site *SiècleDigital*.

[24] Alice VITARD – « Bientôt un parquet national spécialisé dans la cybercriminalité ? ». Mai 2021 ; publié sur le site de *l'Usine Digitale* – Op.cit

LA CRISE SANITAIRE MONDIALE, UN CONTEXTE FAVORABLE À LA CYBERCRIMINALITÉ

Par **Vincent LE TROUHER /** CHARGÉ DE MISSION LUTTE CONTRE LA FRAUDE, ENTREPRENEUR, AUTEUR DE « DROIT PÉNAL DES AFFAIRES ET GROUPES DE SOCIÉTÉS – UNE SOUPLESSE PROPICE AUX INFRACTIONS ET À L'IMPUNITÉ » (L'HARMATTAN).

OBSERVATOIRE DES CRIMINALITÉS INTERNATIONALES / JANVIER 2022
Sous la direction de Gaëtan Gorce et David Weinberger, chercheur associé à l'IRIS
ObsCI@iris-france.org

L'ObsCI a pour objectif d'étudier et d'analyser les différents champs des criminalités internationales en appréhendant les problématiques sécuritaires dans leur globalité, en intégrant ses enjeux pour nos sociétés et leurs effets sur les politiques publiques en France comme à l'international.

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES
2 bis rue Mercœur
75011 PARIS / France

T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org