Formation Continue
Université de Strasbourg

Année universitaire 2023-2024

Master 2 de Droit pénal des affaires mention Investigations financières à l'échelle européenne (IFEE)

Mémoire présenté par :
Mathieu HAN-LEVEAU

Les fuites de données : un bon tuyau ?

-

Etude juridique sous le prisme de l'investigation financière des données issues de cyberattaques aux rançongiciels

Mémoire dirigé par :

- Madame Chantal CUTAJAR, maître de conférences à l'Université de Strasbourg, habilité à diriger des recherches (HDR).

- Monsieur Marc SIMON, chef du service analyse criminelle opérationnelle de la police fédérale Belge.

« Everyone is hackable » [1]

—

APPIN SECURITY, société spécialisée dans le *hack for hire*

« *On n'échappe à rien, pas même à ses fuites* »

—

Jean-Jacques Goldman : « *On ira* » (1997)

[1] *https://www.documentcloud.org/documents/22065658-appin-efiia-pp page 24*

REMERCIEMENTS

Je tiens à adresser mes remerciements à :

Madame Cutajar et Monsieur Simon pour avoir été mes tuteurs dans le cadre de la rédaction de ce mémoire.

L'ensemble du personnel pédagogique de l'Université de Strasbourg, et en particulier Emilie Ehrengarth pour son expertise et sa bonne humeur tout au long de l'année.

Christophe, pour son aide de franc-tireur ainsi qu'à ma collègue Nolwenn pour son soutien.

Ma famille et à ma compagne Zoé, pour ses conseils justes et éclairés.

*

* *

LISTE DES ACRONYMES :

AFC : Analyse financière criminelle
ANSSI : Agence nationale de la sécurité des systèmes d'information
ART : Article
BGH : Big Game Hunting
BRIF : Brigade de recherches et d'investigations financières
CA : Chiffre d'affaires
CANAFE : Centre d'analyse des opérations et déclarations financières du Canada
CDI : Captation de données informatiques
CEDH : Cour européenne des droits de l'Homme
CIETAC : Commission Chinoise d'Arbitrage de l'Économie et du Commerce International
CNIL : Commission nationale de l'informatique et des libertés
CNRTL : Centre national de ressources textuelles et lexicales
CP : Code pénal
CPP : Code de procédure pénal
DNEF : Direction Nationale des enquêtes fiscales
DNRED : Direction nationale du renseignement et des enquêtes douanières
DNS : Domain Name Server
ETNC : États et territoires non coopératifs
FBI : Federal Bureau of Investigation
FOVI : Faux ordres de virements
GAFI : Groupe d'action financière
GRU : Glavnoïé Razvédyvatel'noïé Oupravlénié
IANA : Internet assigned numbers authority
IFC : Investigation financière criminelle
LOPMI : Loi d'orientation et de programmation du ministère de l'intérieur
NDA : Non Disclosure Agreement
OCCRP : Organized crime and corruption reporting project
OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
OFEV : Office fédéral de l'environnement
OPCW : Organisation pour l'interdiction des armes chimiques
OSINT : Open-Source intelligence
PDG : Président directeur général
PM : Personnes morales
PPE : Personnes politiquement exposées
RAAS : Ransomware As a Service
RDI : Recueil de données informatiques

RTS : Radio Télévision Suisse
SGDSN : Secrétariat général de la défense et de la sécurité nationale
SNDJ : Service d'enquêtes judiciaires des finances (SEJF)
STAD : Système de traitement automatisé de données
STNCJ : Service technique national de captation judiciaire
TLD : Top level domain
TOR : The onion routeur
TSMC : Taiwan Semiconductor Manufacturing Company
UE : Union Européenne
USA : États-Unis D'Amérique

Formation Continue
Université de Strasbourg

SOMMAIRE

INTRODUCTION

Les fuites de données informatiques, de plusieurs natures, et communément désignées par leurs noms anglais *leaks*, sont souvent présentées comme un enjeu de cybersécurité. Popularisées depuis la création des sites WIKILEAKS et CRYPTOM, elles sont aussi utilisées comme vecteur de diffusion dans le cadre de revendications militantes.

Elles constituent néanmoins une source d'information gagnant en popularité dans les milieux du journalisme d'investigation et des cabinets de renseignement privé / d*ue diligence*. Les *leaks* peuvent survenir de plusieurs manières, via des lanceurs d'alerte, par vengeance ou mauvaise configuration de serveurs informatiques ou par des campagnes de « piratage et diffusion » plus connues sous le nom anglais de « *Hack and Leak Opperations* ». Les fuites de données ont été étudiées ces dernières années par plusieurs journalistes et chercheuses notamment sous l'angle des campagnes d'influence[2], de l'archivage[3], de procès criminels[4] ou commerciaux[5] aux États-Unis d'Amérique, ainsi que sous l'angle scientifique[6] et même culinaire[7]. Ces ouvrages se focalisent essentiellement sur des fuites de données émanant de lanceurs d'alertes ou d'« hacktivistes » et diffusées de manière large sur internet.

En revanche, peu de sources adoptent l'angle de l'investigation financière et cherchent à se focaliser sur les fuites de données issues de groupe cyber rançonneurs plus spécifiquement, et diffusés de manière plus restreinte sur internet.

---

[2] *Vasset, Philippe, et Pierre Gastineau. Armes de déstabilisation massive. Paris: Fayard, 2017.*

[3] *Somé-Blad, Elodie. « Du leak en tant qu'archive, ou comment le leak est devenu une archive ». Université de Lyon, 2017. https://www.enssib.fr/bibliotheque-numerique/documents/67750-leak-en-tant-qu-archive-ou-comment-le-leak-est-devenu-une-archive-du.pdf.*

[4] *Freeman, Lindsay. « Hacked and Leaked: Legal Issues Arising From the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases ». UCLA Journal of International Law and Foreign Affairs, Human Rights Center, UC Berkeley School of Law, 25, no 2 (2021): 45-91. https://escholarship.org/content/qt5b87861x/qt5b87861x_noSplash_48c123785a2ad83b4be92dd72497af91.pdf.*

[5] *Yenouskas, Joseph F, et Levi W Swank. « Emerging Legal Issues in Data Breach Class Actions ». The Business Lawyer 73, no 2 (2018). https://www.americanbar.org/groups/business_law/resources/business-law-today/2018-july/emerging-legal-issues-in-data-breach-class-actions/.*

[6] *Bertran, Marie-Gabrielle. « Illustration des apports et limites de l'usage des sources ouvertes à travers le cas de la Russie ». Hérodote 186, no 3 (2022): 85-99.*

[7] *Glace, Demetria. Leaked recipes: the cookbook. JBE <3 food. Paris: JBE books, 2020.*

Ces fuites de données, provenant en grande majorité d'entreprises, sont mises à disposition par les pirates informatiques sans restrictions, gratuitement et de manière native [8].

Imaginons maintenant qu'un cabinet d'avocat situé dans une juridiction « *offshore* » et spécialisé dans l'aide à l'évasion fiscale de personnalités politiques ait été attaqué par des cyber corsaires. Aprés avoir refusé de payer le prix fort, l'ensemble de ses données les plus sensibles sont publiées en ligne. Pour tout enquêteur financier, cela s'apparente à une véritable aubaine dans son expédition entre les flots des vaisseaux amiraux des cabinets d'avocats fiscalistes, les cuirassés des pays et territoires non coopératifs et les navires fantômes des sociétés de domiciliation.

Pour autant, peut-on verser en procédure ces données dans le cadre d'une affaire pénale sans risquer l'avarie ? Cela vaut-il le coup de s'y risquer ? D'autres l'ont-ils déjà fait auparavant ? Peut-ont quand même les utiliser ?

Ce mémoire a pour ambition de passer à l'abordage ces questions par le biais d'une étude théorique et pratique sous le prisme du droit pénal, de l'investigation financière et de la cybercriminalité.

[8] *Les fuites de données issues de lanceurs d'alertes, comme les OFFSHORE LEAKS, sont pour leurs part mises à disposition via des synthèses relationnelles (noeuds, liens) ou des base de données orientée graphe. Bien que les journalistes disposent des données originelles (facture, email par exemple) ainsi que leurs métadonnées, elle ne sont pas rendues publiques.*

DÉFINITIONS

A. Fuite de données

Pour l'heure, il n'existe pas de définition juridique et unanimement partagée concernant les « fuites de données ». La seule définition pouvant correspondre à l'axe de recherche de ce mémoire serait celle de la « violation de données » précisée par la Commission nationale de l'informatique et des libertés (CNIL) et intimement liée aux données à caractères personnels : « *Une violation de la sécurité se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles* ». La fuite quant à elle est définie par le Centre national de ressources textuelles et lexicales (CNRTL)[9] Comme étant la « *Mise à jour, divulgation de documents qui auraient dû rester secrets* ». Il définit par ailleurs la « donnée » comme « *L'ensemble des indications enregistrées en machine pour permettre l'analyse et/ou la recherche automatique des informations* ».

L'alliance de ces définitions juridico-techniques permet de définir les fuites de données comme étant la divulgation, volontaire ou involontaire, de données privées présentes sur un système de traitement automatisé de données (STAD).

[9] *Le Centre national de ressources textuelles et lexicales est une organisation française qui diffuse en ligne des données linguistiques. Créé en 2005 par le CNRS, le CNRTL fédère au sein d'un portail unique, un ensemble de ressources linguistiques informatisées et d'outils de traitement de la langue.*

B. Rançongiciel

Un rançongiciel, plus connu sous la dénomination anglaise de « *ransomware* », est selon l'agence nationale de la sécurité des systèmes d'information (ANSSI)[10] :

« un *programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. (...) Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon. Lorsqu'un rançongiciel infecte un poste de travail, le plus souvent (mais pas nécessairement) par l'envoi d'un courrier électronique piégé, l'infection est dès lors susceptible de s'étendre au reste du système d'information (serveurs, ordinateurs, téléphonie, systèmes industriels, etc.)*[11] ».

C. Investigation financière

L'investigation/enquête[12] financière désigne un panel de mesures techniques permettant de détecter des flux financiers issus d'activités illicites, de leurs blanchiments et de l'achat ou de la vente de biens mal acquis via ces mêmes activités. Comme le précise Elena Addesa-Pelliser dans sa thèse[13], l'investigation financière n'a pas de définition stricte en droit français ou européen. Seules des mesures techniques sont explicitées pour la première fois en 1990 aux articles 3 et 4 de la convention du Conseil de l'Europe de 1990 relative au blanchiment, au dépistage, au gel, à la saisie et à la confiscation des produits du crime. Également appelé STE 141, cette convention indique en son article 4 que :

« *Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses tribunaux ou ses autres autorités compétents à ordonner la communication ou la saisie de dossiers bancaires, financiers ou commerciaux afin de mettre en œuvre les mesures visées aux articles 2 et 3. Une partie ne saurait invoquer le secret bancaire pour refuser de donner effet aux dispositions du présent article. Chaque Partie envisage d'adopter les mesures*

---

[10] Service dépendant du secrétariat général de la défense et de la sécurité nationale (SGDSN), l'ANSSI à pour mission de défendre les systèmes d'information de l'État et également d'apporter une expertise et un soutien aux administrations et aux opérateurs d'importance vitale.

[11] https://www.ssi.gouv.fr/entreprise/glossaire/r/ consulté le 5 juillet 2023.

[12] Le mot investigation étant l'anglicisme du mot français enquête.

[13] Addesa-Pelliser, Elena. « Le Gafi, l'investigation financière criminelle (IFC) et l'analyse financière criminelle (AFC) : un changement paradigmatique à l'oeuvre. » Université de Strasbourg, 2019. https://theses.hal.science/tel-03525636/document.

législatives et autres qui se révèlent nécessaires pour lui permettre d'employer des techniques spéciales d'investigation facilitant l'identification et la recherche du produit ainsi que la réunion de preuves y afférentes. Parmi ces techniques, on peut citer les ordonnances de surveillance de comptes bancaires, l'observation, l'interception de télécommunications, l'accès à des systèmes informatiques et les ordonnances de production de documents déterminés. »[14]

Cité de manière plus précise et récente, l'investigation/enquête financière apparaît dans les recommandations du GAFI formulées en 2012[15]:

« *Financial investigation involves the collection, collation and analysis of all available information with a view towards assisting in the prosecution of crime and in the deprivation of the proceeds and instrumentalities of crime. Criminals usually like to maintain some degree of control over their assets, and as a result there is usually a "paper trail" that will lead back to the offender.That paper trail can also be followed to identify additional offenders and potentially the location of evidence and instrumentalities used to commit the crimes. The ability of law enforcement agencies to conduct financial investigations and have access to financial and other information is essential to effectively combating ML, associated predicate offences and TF offences(..) Financial enquiries are often intrusive and result in obtaining private information on an individual. Competent authorities involved in financial investigations must be aware of their country's human rights legislation protecting the right to privacy, along with associated considerations.*[16]. »

---

[14] *Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime du 9 novembre 1990 (1990). https://rm.coe.int/168007bd2f.*

[15] *« GAFI/FATAF:Operational Issues - Financial Investigations Guidance », juin 2012. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf.*

[16] *Traduction du rédacteur. :*

« Une enquête financière implique la collecte, le rassemblement et l'analyse de toutes les informations disponibles en vue d'aider à la poursuite des infractions et à la confiscation des produits et instruments du crime. Les criminels gardant un certain degré de contrôle sur leurs actifs et leurs biens, il existe par conséquent, généralement une "trace écrite" qui permet de remonter jusqu'à l'auteur de l'infraction. Cette trace écrite peut également être suivie pour identifier d'autres délinquants et éventuellement l'emplacement des éléments de preuve et des instruments utilisés pour commettre l'infraction. La capacité des services répressifs de mener des enquêtes financières et d'avoir accès à des informations financières et autres est essentielle pour lutter efficacement contre le blanchiment d'argent qui y est associé. (...) Les enquêtes financières sont souvent intrusives et aboutissent à l'obtention d'informations privées sur un individu. Les autorités compétentes impliquées dans les enquêtes financières doivent connaître la législation de leur pays en matière de droits de l'homme qui protège le droit à la vie privée, ainsi que les considérations qui y sont liées »

CHAPITRE I : Le potentiel de des fuites de données issues de rançongiciels

Ce premier chapitre abordera le sujet de ce mémoire sous l'angle de l'investigation. En premier lieu il convient de bien cerner la réalité des attaques par rançongiciels (section 1) afin de savoir, dans un second temps, si des enquêtes ont déjà été menées sur cette base ainsi que les moyens permettant d'identifier des données d'intérêt (section 2).

Section 1 : Évolution et tendances des rançongiciels

Longtemps cantonnée à des sites ou comptes Twitter spécialisés, la thématique des rançongiciels contamine désormais les principaux quotidiens nationaux[17], notamment suite à des attaques touchant des hôpitaux. En novembre 2022 le journal LIBÉRATION lui consacre même la une de son édition en ligne[18], et le département de la justice des États-Unis D'Amérique (USA) sa plus grosse récompense, 10 millions de dollars[19], jadis consacrés presque exclusivement aux terroristes. Loin de la hâte des salles de rédaction et leurs titres d'article plus ingénieux les uns que les autres, un panorama synthétique et factuel au sujet des rançongiciels s'impose.

A. Des Arsène Lupin devenus de véritables *condottières* du cybercrime

1. La genèse du racket en ligne

Les rançongiciels et les administrateurs systèmes ont récemment fêtés leurs noces de perles. En effet, le premier cybercorsaire connu pour avoir usé de rançongiciels fut Joseph POPP[20] qui lança le maliciel AIDS en 1989. Contraignant ses victimes par un chiffrement symétrique de leurs données[21], les

---

[17] 799 occurrences sur le site internet du quotidien LE MONDE et 775 pour celui du LE FIGARO

[18]Guiton, Amaelle. « Rançongiciels: un chantage qui chiffre sérieusement ». Libération, 22 novembre 2022. https://www.liberation.fr/societe/rancongiciels-un-chantage-qui-commence-a-serieusement-chiffrer-20221123_CABNEQARZBH5JLNASFGVESFFNI/.

[19] Department of Justice. « Rewards for Justice Up to $10 million », s. d. https:// rewardsforjustice.net/rewards/conti/.

[20] Murphy Kelly, Samantha. « The bizarre story of the inventor of ransomware ». CNN Business, 16 mai 2021. https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html.

[21] Symétrique uniquement. L'utilisation de chiffrement asymétrique tel qu'utilisé aujourd'hui par les rançongiciels a été identifié comme intéressant d'un point de vu offensif en 1996. Voir à ce sujet: IEEE Computer Society, International Association for Cryptologic Research, et Institute of Electrical and Electronics Engineers, éd. Cryptovirology : Extortion-Based Security Threats and Countermeasures. Los Alamitos, Calif.: IEEE Computer Society Press, 1996. https://www.ieee-security.org/TC/SP2020/tot-papers/young-1996.pdf.

rendant donc inutilisables, le maliciel réclamait un paiement de 186 $ pour les libérer du joug du procédé cryptographique. Ce virus informatique est bien la première forme de rançongiciels connue à ce jour. Après quelques balbutiements dans leurs utilisations par des acteurs malveillants de manière isolée, un tournant s'opère en 2013 lorsque se propage CRYPTOLOCKER[22]. Ce rançongiciel avait effectivement pour particularité d'opérer via un chiffrement asymétrique et d'exiger un paiement des rançons en BITCOIN[23]. L'utilisation de ces deux mécanismes offrant d'une part un chiffrement plus robuste, et donc plus contraignant pour les victimes, ainsi qu'un mode paiement éloigné du secteur financier traditionnel, et donc plus difficilement traçable que les cartes prépayées ou coupons utilisés jusqu'alors, ont attirés l'attention de nombreux pirates informatiques. Les sommes soutirées, de plus en plus importantes[24], ont convaincues les derniers sceptiques, au point même que certains États sous embargo international les utilisent pour financer leurs programmes de prolifération nucléaire et balistique comme la Corée du Nord avec le virus WANA-CRY[25].

Aujourd'hui tournés sur un modèle de franchise, baptisé RAAS pour « *Ransomware As a Service* », les acteurs malveillants développent ces logiciels ainsi que les chaînes de paiement en cryptoactifs et les mettent à disposition d'attaquants spécialisés dans la pénétration de systèmes informatiques.
Les rançons perçues sont ensuite réparties entre les développeurs et les attaquants suivant un modèle propre à chaque entité[26].

---

[22] https://ucr.fbi.gov/washingtondc/news-and-outreach/press-room/this-month/this-month-at-the-wfo-june-2014.pdf

[23] Crypto-actifs reposant sur la technologie blockchain pouvant être échangé contre des monnaies ayant cours légal ou bien simplement pour effectuer des achats.

[24] Plus de 27 millions de dollars pour crypto-locker selon le FBI. Voir : FBI Press room. « FBI Leads Action Against "CryptoLocker" Ransomware », juin 2014. https://ucr.fbi.gov/washingtondc/news-and-outreach/press-room/this-month/this-month-at-the-wfo-june-2014.pdf F.

[25] United States of America VS PARK JIN HYOK, also known as (« aka »), « Jin Hyok Park, » aka « Pak Jin Hek, » No. M18- 1479 (s. d.).

*[26] Selon lui rapport de l'entreprise suisse, PRODAFT, spécialisée dans la protection informatique les commission pour les affiliées varient entre 10 et 30% du montant total de la rançon.
Voir : Prodaft. « Conti Ransomware Group In-Depth Analysis ». Cyber. Suisse: PRODAFT, s. d. https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf.*

2. Un secteur dynamique ciblant principalement les entreprises à forte croissance

Il convient tout d'abord de rappeler que la quantification du nombre d'attaques informatiques via les rançongiciels est un exercice compliqué. Effectivement, la majorité des rapports publiés par les firmes de cybersécurité ou les agences publiques en charge de la protection du cyberespace fondent leurs analyses tendancielles sur le nombre de victimes publié sur les sites des groupes cybercriminels ou bien par le nombre plaintes déposées, en France via l'application THESSE dédiée aux arnaques sur internet[27].

La loi LOPMI[28] et plus particulièrement son chapitre X implique effectivement un dépôt de plainte afin d'activer les clauses d'un contrat d'assurance visant à indemniser les risques cyber. Ainsi, les attaques n'ayant pas abouti, ou celles pour lesquelles l'entreprise a payé la rançon ne figurent donc pas forcément dans la liste des victimes sur les sites des attaquants. Il en est de même pour les entreprises n'ayant pas déposé plainte, car n'ayant pas souscrit à une assurance couvrant les risques cyber, et qui sont donc éludés du calcul. Partant de ce postulat et en gardant ces précautions en tête, les attaques aux rançongiciels semblent avoir baissé en nombre en France, de 46 % entre 2021 et 2022 selon l'ANSSI [29], et en volume au niveau mondial, soit de 4 % selon l'entreprise américaine IBM[30].

---

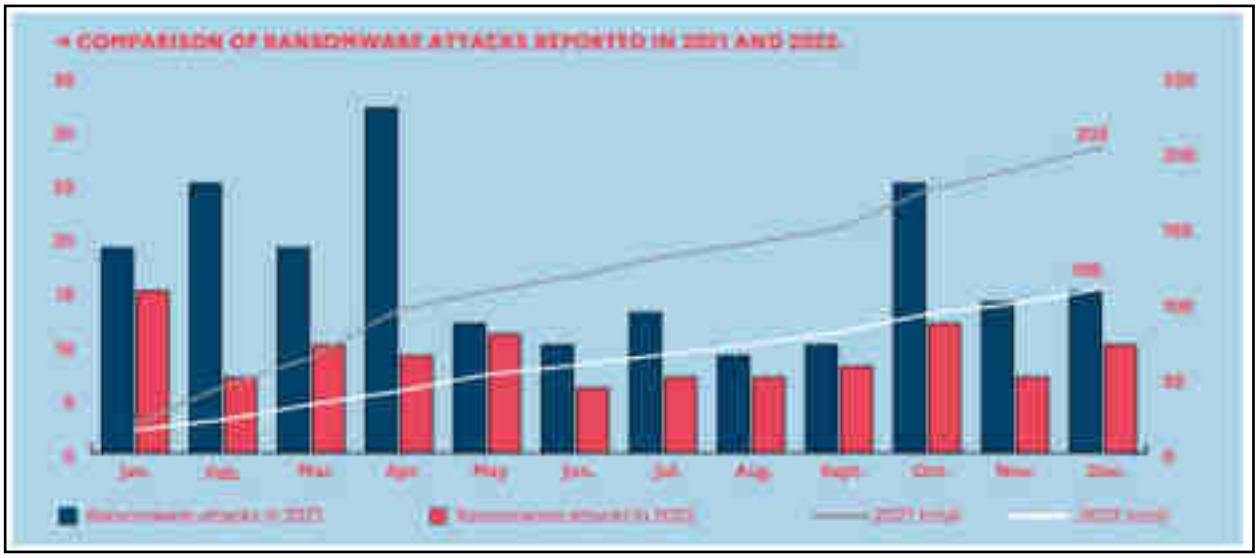
[27] Direction de l'information légale et administrative (Première ministre). « Ransomware ou rançongiciel ». service-public.fr (blog), 15 mars 2022. https://www.service-public.fr/particuliers/vosdroits/F34129.

[28] LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, IOMD2223411L § (2023). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768.

[29] « CYBER THREAT OVERVIEW 2022 ». Rapport annuel. Paris: Agence nationale de la sécurité des systèmes d'information, janvier 2023. Page 15. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf.

[30] « Definitive guide to ransomware 2023 ». IBM SECURITY, mai 2023. Page 4. https://www.ibm.com/downloads/cas/OW1D41LK.

Le gouvernement des USA observe cependant une hausse des attaques visant ses instituons ou les entreprises implantées sur son territoire[31].



(*Évolution du nombre d'attaques détectées par l'ANSSI en France entre 2021 et 2022* [32])

Au point de vue tendanciel, le secteur semble s'orienter ver une « chasse au gros poisson » (Big Game Hunting / BGH en anglais) privilégiant les attaques ciblées sur des entreprises ayant d'importants chiffres d'affaires (CA) auxquelles ils peuvent demander une plus grande rançon, en les privant parfois totalement de leurs activités[33] et portant atteinte à leurs réputations et à leurs niveaux de sécurité vis-à-vis de leurs fournisseurs et clients. Ces entreprises sont donc bel et bien des cibles de choix, comme en atteste la récente attaque perpétrée en juillet 2023 à l'encontre d'un fournisseur de Taiwan Semiconductor Manufacturing Company (TSMC) avec une rançon s'élevant à 70 millions de dollars.

---

[31] « 2021 Trends Show Increased Globalized Threat of Ransomware ». Cybersecurity and Infrastructure Security Agency (CISA), février 202apr. J.-C. https://www.cisa.gov/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf.

[32] CYBER THREAT OVERVIEW 2022 ». Rapport annuel. Paris: Agence nationale de la sécurité des systèmes d'information, janvier 2023. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf. page 15

[33] ZDNET. « Un constructeur aéronautique paralysé par un ransomware », 13 juin 2019. https://www.zdnet.fr/actualites/un-constructeur-aeronautique-paralyse-par-un-ransomware-39885909.htm.

Le nombre de groupe cybercriminels utilisant des rançongiciels est lui aussi en augmentation[34], notamment suite à la dislocation du CONTI GANG[35] et au démantèlement de l'infrastructure du groupe HIVE par le FBI et EUROPOL[36]. Jadis les Messi et Ronaldo du racket en ligne, ces deux groupes figuraient parmi le top 3 des attaquants ayant engrangé le plus de revenus en 2021. Leurs disparitions ont laissé plus de part de marché aux acteurs en place et à ceux hésitant à se lancer. Plus encore, la diffusion involontaire du code source de ces logiciels ainsi que de leurs manuels internes comme cela fut le cas pour CONTI et LOCKBIT 3.0[37], à sans aucun doute mit le pied à l'étrier aux pirates informatiques hésitant encore à se lancer dans les rançongiciels. En janvier 2023, la société MICROSOFT affirmait avoir identifié plus de 100 groupes cyber rançonneurs [38].

B. Un nouveau moyen de pression à l'origine d'un tsunami de données

Face à cette menace informatique, des contremesures et des préconisations ont été développées par les gouvernent et les entreprises spécialisés dans la protection informatique[39]. Comme le précise l'ANSSI dans un rapport publié en 2020 « *L'objectif principal d'un rançongiciel est d'empêcher la victime d'accéder à ses données, le plus souvent par le chiffrement de ces dernières.*

---

[34] Wagner Ramsdell, Kellyn A, et Kristin E. Esbeck. « EVOLUTION OF RANSOMWARE ». The MITRE Corporation, juillet 2021.

Threat & Detection Research Team. « État des lieux de la menace Ransomware au second semestre 2022 ». SEKOIA.IO, 31 janvier 2023. https://blog.sekoia.io/fr/etat-des-lieux-de-la-menace-ransomware-au-second-semestre-2022-par-sekoia-io/.

[35] Cox, Joseph. « Pro-Russia Conti Ransomware Gang Targeted, Internal Chats Leaked ». VICE MAGAZINE, 28 février 2022. https://www.vice.com/en/article/z3ng84/pro-russia-conti-ransomware-messages-leaked.

[36] EUROPOL. « Cybercriminals stung as HIVE infrastructure shut down », 26 janvier 2023. https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.

[37] S. Alzahrani, Y. Xiao and W. Sun, "An Analysis of Conti Ransomware Leaked Source Codes," in IEEE Access, vol. 10, pp. 100178-100193, 2022, doi: 10.1109/ACCESS.2022.3207757. + https://intel471.com/blog/lockbit-3-0-builder-code-leak-points-to-another-disgruntled-criminal-employee

[38] Microsoft Threat Intelligence. TWITTER (blog), janvier 2023. https://twitter.com/MsftSecIntel/status/1620474448494075909?lang=fr.

[39] Agence nationale de la sécurité des systèmes d'information. « Attaques par rançongiciels, tous concernés. », 4 septembre 2020. https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes.

Orange Cyberdéfense. « Beating ransomware A comprehensive guide to tackling the cyber extortion threat », 2021. https://www.orange-business.com/sites/default/files/beating-ransomware-solutions-guide.pdf.

Devant cette menace, la réalisation de sauvegardes régulières des données apparaît comme la mesure prioritaire pour réduire les pertes liées à une attaque par rançongiciel »[40] . Ne dérogeant pas au principe historique de la course entre le blindage et la munition, les acteurs malveillants ont mis leur créativité en ébullition face à la recrudescence des sauvegardes de secours isolées déployées par les entreprises. C'est ce nouveau moyen de pression des cyber rançonneurs qui constitue la pierre angulaire de ce mémoire.

1. Un chantage à la publication

Désormais, les données ne sont plus uniquement chiffrées, mais aussi dérobées par les cyber rançonneurs. Les entreprises sont par la suite menacées d'une diffusion en ligne de leurs informations, en grande majorité sur le réseau TOR[41]. Ce réseau est accessible via le navigateur TOR BROWSER[42] conçu, entre autres, pour accéder aux « *onions services* » qui sont des sites internet reconnaissables à leurs extensions de domaine en « . onion ». Techniquement, il s'agit d'un réseau informatique superposé[43] à internet (*overlay network*), souvent appelé « *dark net* » dans les médias. Les rançongiciels mettant en œuvre cette tactique ont été qualifiés de « rançongiciels à double extorsion »[44].

L'ANSSI en fait ainsi mention pour la première fois dans un rapport publié en janvier 2020 et date leurs apparitions à novembre 2019 :

« *Le principe de double extorsion existe depuis novembre 2019 et aurait été introduit par les opérateurs du rançongiciel Maze. Il consiste à faire pression sur la victime en exfiltrant ses données et en la menaçant de les publier sur un site Internet, généralement en .onion, dans le but qu'elle paye la rançon. Cette menace est limitée dans le temps. Par exemple, les opérateurs d'Egregor laissent aux victimes un délai de 72 heures pour les contacter, sans quoi leurs données sont publiées »*[45].

---

[40] *ibid*

[41] *Réseaux crée afin de garantir un certain anonymat lors de la navigation en ligne notamment via la fonctionnalité des « Hidden services »* https://www.torproject.org/fr/about/history/

[42] *Utilisé par environs 2,5 millions de personnes dans le monde en 2022 : « TOR METRICS USERS », 22 novembre 2023. https://metrics.torproject.org/userstats-relay-country.html?start=2022-01-01&end=2022-12-31&country=all&events=off.*

[43] *Lua, Eng Keong, Jon Crowcroft, Marcelo Pias, Sharma Ravi, et Lim Steven. « A Survey and Comparison of Peer-to-Peer Overlay Network Schemes ». IEEE COMMUNICATIONS SURVEY AND TUTORIAL, 31 mars 2004. https://snap.stanford.edu/class/cs224w-readings/lua04p2p.pdf.*

[44] *Cybersecurity and Infrastructure Security Agency. « #StopRansomware Guide », s. d. https://www.cisa.gov/stopransomware/ransomware-guide.*

[45] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

Depuis, ce sont plusieurs centaines de milliers de gigaoctets qui ont été déversés en ligne par les cyberrançonneurs. À titre d'exemple, l'attaque perpétrée par le groupe LOCKBIT à l'encontre de la société allemande Continental, spécialisée dans le domaine automobile, s'est soldée par la publication de 400 000 gigaoctets (40 téraoctets) de données internes à l'entreprise[46].

2. Des données sensibles à portée de clic

Parmi les données siphonnées figurent parfois des documents personnels, comme des échanges entre des avocats et leurs clients[47] ; des informations sensibles telles que des listes de fournisseurs[48] ; des brevets en cours d'élaboration[49] ; des accords de non-divulgation (non-disclosure agrément)/NDA[50] ; et même parfois des données classifiées[51]. Les sites de ces cybercorsaires en regorgent par centaines de giga-octets.

À titre d'illustration, il est possible de citer le cas de l'entreprise indienne SOLAR INDUSTRIES œuvrant dans le domaine militaire et attaqué par le groupe cybercriminel ALPHV[52], qui a publié des échantillons des données sur

---

[46] Glover, Claudia. « FBI joins investigation into Continental ransomware attack ». TECHMONITOR.AI (blog), 23 novembre 2022. https://techmonitor.ai/technology/cybersecurity/continental-cyberattack-ransomware-lockbit-fbi.

[47] Bogdan, Bodnar. « Les avocats de plus en plus ciblés par les hackers, alerte l'ANSSI ». Numérama (blog), 27 juin 2023. https://www.numerama.com/cyberguerre/1428430-les-avocats-de-plus-en-plus-cibles-par-les-hackers-alerte-lanssi.html.

[48] Hope, Alicia. « United States Nuclear Missile Contractor Hit by Maze Ransomware Attack ». CPO magazine (blog), s. d. 11 juin 2020.

[49] Page, Carly, et Zack Whittaker. « Hackers publish sensitive employee data stolen during CommScope ransomware attack ». TechCrunch (blog), 17 avril 2023. https://techcrunch.com/2023/04/17/hackers-publish-sensitive-employee-data-stolen-during-commscope-ransomware-attack/.

@FalconFeedsio. Twitter (blog), 28 octobre 2022. https://twitter.com/FalconFeedsio/status/1585868867817312256.

[50] Abrams, Lawrence. « Computer hardware giant GIGABYTE hit by RansomEXX ransomware ». Bleeping Computer (blog), s. d. https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/.

[51] « The Anatomy of Targeted Ransomware Attacks ». Danish Centre for Cybersecurity, 16 novembre 2020. https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/cfcs-the-anatomy-of-targeted-ransomware-attacks.pdf.

[52] Paganini, Pierluigi. « BlackCat Ransomware gang stole secret military data from an industrial explosives manufacturer ». Security Affairs (blog), 27 janvier 2023. https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html.

son site, tel que des dessins techniques, des spécifications d'ingénieurs, ou des rapports d'audit.

(Source : https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html)

Dans un contexte économique fortement concurrentiel et en se référant aux théories économiques sur les marchés avec asymétrie d'information, — en particulier ceux relatifs à l'information privée et aux théories du « *screening* » de Joseph Stiglitz[53] — la divulgation de ces données commerciales et technologiques peut grandement nuire à une entreprise, de même que favoriser celles qui n'hésiteraient pas à les consulter.

[53] *Le screening est une théorie ayant pour objectif d'expliquer le processus qui permet d'obtenir l'information privée (information privilégiée) de la part d'un agent économique. C'est l'une des composantes de base de l'économie de l'information, avec le Market for Lemons d'Akerlof (asymétrie d'information). A ce sujet voir : Stiglitz, J. E. (1975). The Theory of "Screening," Education, and the Distribution of Income. The American Economic Review, 65(3), 283–300. http://www.jstor.org/stable/1804834*

Section 2 : Cybercriminels et investigations : les rançonneurs apportent leur pierre à l'édifice

Comme explicité auparavant, les entreprises qui ne s'acquittent pas du paiement de la rançon sont « punies » par les pirates informatiques qui les diffusent alors sur leur site internet, bien souvent via les « *hidden services* » du réseau TOR. La fuite de données ruisselle désormais en ligne aux yeux de tous. Peu de doutes résident sur le fait que ces données soient une aubaine pour d'autres pirates informatiques, ou malfaiteurs en tout genre souhaitant recycler ces informations et documents à des fins de cyber hameçonnage (*phishing/spear phishing*), d'usurpation d'identité, faux ordres de virements (FOVI), de même que pour des sociétés concurrentes

En chien de faïence des opens-spaces des branches « recherches et développement » « sécurité » ou « *due dilligence* » d'entreprises s'attelant à rester le mieux informer sur leurs concurrents[54], les bureaux feutrés des salles de rédaction et ceux cloisonnés des services d'enquêtes nationaux cherchent eux aussi, et à leur manière, à être le mieux renseigné possible. Ces derniers travaillent depuis de nombreuses années par le biais de leurs vecteurs de prédilection : source humaine et OSINT pour les journalistes, droit de communication, réquisition, courrier de dénonciation souvent farfelu et perquisition pour les services de l'Etat. Il est possible d'identifier que ces fuites de données issues d'attaques aux rançongiciels ont déjà été utilisées lors d'investigations (A) et qu'une méthodologie de recherche propre à ce vecteur d'information peut être mis en place (B).

A. Une martingale utilisée par les journalistes

1. Les sociétés offshores des oligarques russes exposés au grand jour

C'est par le journal LE TEMPS[55] et sous le clavier du journaliste helvétique Sébastien Ruche qu'apparaît explicitement, le 21 avril 2022, la première enquête reposant sur des données diffusées par des cyber rançonneurs. Dans son article intitulé « *Des hackers russes dévoilent par mégarde les données de plusieurs oligarques* »[56] le journaliste s'appuie sur des documents internes de la société

[54] *Voir à ce sujet le livre du journaliste Matthieu Suc : Suc, Matthieu. Renault, nid d'espions. Poche 205. Paris: Harper Collins, 2020.*

[55] *LE TEMPS est un quotidien suisse basé à Genève propriété de la fondation a but non lucrative Aventinus*

[56] *Ruche, Sébastien. « Des hackers russes dévoilent par mégarde les données de plusieurs oligarques ». LE TEMPS (blog), 21 avril 2022. https://www.letemps.ch/economie/finance/hackers-russes-devoilent-megarde-donnees-plusieurs-oligarques.*

fiduciaire caïmanaise GENESIS TRUST & CORPORATE SERVICES publiés par le groupe LOCKBIT 2.0, un des ténors du crime en ligne. Le quotidien genevois affirme avoir consulté certains de ces 84 500 fichiers, notamment des « *Organigrammes, e-mails, contrats, communications avec des banques, copies de passeports, rapports en tout genre »* et affirme à l'appui que cette dernière aurait créé des structures *offshores* pour des personnes politiquement exposées (PPE) et des oligarques russes sous sanctions internationales, tels que Suleiman Abusaidovich Kerimov[57].

Un second article publié cinq mois plus tard dans le même journal par les journalistes Marc Gueniart et Antoine Harar en partenariat avec l'Organized Crime and Corruption Reporting Project (OCCRP), affirme que les documents dévoilés par LOCKBIT 2.0 ont permis de compléter le puzzle d'informations sur les avoirs de l'oligarque ainsi que sur le rôle joué par sa proche famille[58]. Les journalistes pointent notamment qu'un flux financier de 400 millions de dollars américains aurait été effectué en 2014 par les enfants de Mr Kerimov, Gulnara Kerimova et Saïd Kerimov, via GENESIS TRUST & CORPORATE SERVICES, pour abonder la société suisse HUMAN DIVERSITY FOUNDATION détenue par Suleiman Abusaidovich Kerimov. Plus encore ces données exposeraient le rôle central de Markus Linder dans ces manœuvres :

« *Ces documents révèlent le rôle, jusqu'ici resté secret, que joue Markus Linder dans la galaxie Kerimov, qui s'étend bien au-delà de la présidence de Sunset Properties. En 2017, l'essentiel des actifs financiers de la fondation est transféré vers une société des îles Vierges britanniques, Definition Services. À ce moment-là, cette firme a pour directeur le neveu de Kerimov, Nariman Gadzhiev, qui y verse d'ailleurs 251 millions de dollars. Mais depuis l'an dernier, c'est Markus Linder qui est aux commandes.*

---

[57] Suleiman Abusaidovich Kerimov a été placé sous sanction internationale en 2022 par le NAZK ukrainien, l'Union Européenne et l'OFAC étasunien pour ses liens avec le pouvoir russe et son effort apporté à la guerre en Ukraine déclenchée en février 2022.Voir à ce sujet

Council of the European Union. COUNCIL IMPLEMENTING REGULATION implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, 7125/22 § (2022). https://data.consilium.europa.eu/doc/document/ST-7125-2022-INIT/en/pdf.

« Along the sanctioned persons :KERIMOV Suleyman Abusaidovich », s. d. https://sanctions.nazk.gov.ua/en/sanction-person/741/.

« Sanctions List Search », s. d. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=24325.

[58] Guéniat, Marc, et Antoine Harari. « Le réseau suisse du prince des oligarques ». LE TEMPS (blog), 17 septembre 2022. https://www.letemps.ch/suisse/reseau-suisse-prince-oligarques.

Lequel semble apprécier les services de Genesis Trust, à qui il a confié d'autres sociétés, la plupart liées à des intérêts russes. Pour cela, il a été recommandé par Credit Suisse. »

Ainsi, il a été possible de passer outre le jeu de bonneteau habituellement mis en place par ce type de fiduciaire. Ces informations auraient été difficilement accessibles par les journalistes ou par les services de l'Etat. En effet, les îles Caïmans figuraient jusqu'en octobre 2020 sur la liste des et territoires non coopératifs (ETNC) selon le Conseil de l'UE[59] et sont considérés depuis comme un pays ne se conformant pas encore à toutes les normes fiscales internationales, mais qui s'est engagé à mettre en œuvre des réformes[60].

Autre histoire, même pays, une année plus tard. Police épurée, site internet sobre sur fond blanc immaculé qui rappelle les montagnes enneigées aux portes de Zurich, ville dans laquelle est basée la société FINAPORT. Son logo l'incarne par un trait rouge entre FINA et PORT, la société se veut un embarcadère pour la finance. Il est possible d'en apprendre davantage son credo via son site internet : « *Notre objectif est de préserver le patrimoine et de générer des revenus pour tous nos clients dans le monde entier en nous efforçant d'investir d'une manière hautement éthique et durable — en assurant la sécurité pour les générations à venir.* »[61] Elle s'y décrit également comme « *une société de gestion de patrimoine suisse indépendante et réglementée avec des bureaux en Suisse, à Singapour et au Liechtenstein* ».

Au début de l'année 2023 FINAPORT fût frappée par les foudres du groupe ALPHV qui cambriole sans ménagement ses documents internes. Le 5 février 2023, les données extirpées sont brièvement mises en ligne sur le site d'ALPHV, en toute évidence pour cause de non-paiement de la rançon, avant de disparaître quelques jours plus tard sans explication ni annonce.

---

[59] Pour les Iles Caïman voir : Conseil de l'Union européenne. « Chronologie - liste de l'UE des pays et territoires non coopératifs », 17 octobre 2023. https://www.consilium.europa.eu/fr/policies/eu-list-of-non-cooperative-jurisdictions/timeline-eu-list-of-non-cooperative-jurisdictions/.

Pour les ETNC : pays et juridictions figurant en annexe I du rapport du groupe «Code de conduite fiscalité des entreprises » du Conseil de l'UE (ex-liste noir) voir : Conclusions du Conseil relatives à la liste révisée de l'UE des pays et territoires non coopératifs à des fins fiscales (2023). https://data.consilium.europa.eu/doc/document/ST-6375-2023-INIT/fr/pdf.

[60] Pays et juridiction listés en annexe II du rapport du groupe «Code de conduite fiscalité des entreprises » du Conseil de l'UE (ex-liste grise)

[61] FINAPORT. « OUR MISSION », 1 octobre 2023. https://data.consilium.europa.eu/doc/document/ST-6375-2023-INIT/fr/pdf.

En effet, rien n'est définitif et tout peut se négocier avec les cyber corsaires moyennant paiement, y compris a posteriori pour déchiffrer et supprimer les données publiées[62]. La société suisse s'est ainsi probablement résolue à payer les rançonneurs après avoir constaté l'ampleur de la fuite de données. Tout peut se négocier avec ces cyber Arsène Lupins, ou presque. En effet, rien n'est garanti sur la manière dont seront utilisées ces données par ceux qui les auront récupérées dans l'intervalle. Malheureusement pour FINAPORT elles sont arrivées à l'endroit du cauchemar de toute entreprise souhaitant passer sous les radars : le bureau de journalistes d'investigation. Le 14 septembre 2023, la Radio Télévision Suisse (RTS) publie en partenariat avec l'OCCRP, LE MONDE et le journal allemand DER SPIELGEL, une série d'articles sur la société zurichoise. Un revers pour les deux PDG [63] de FINAPORT, Hellmut Schümperli et Alexei Borissov, qui pensaient sans doute éviter le pire en payant a posteriori la rançon. Afin d'éviter les balles perdues, en particulier lorsque que l'on a des choses à cacher, mieux vaut donc payer en temps et en heure ses cyber-geôliers.

La jadis discrète entreprise est accusée par les journalistes d'investigation, qui s'appuient sur ses propres données internes publiées par le groupe ALPHV, d'avoir manqué à ses obligations en matière de conformité. En particulier, il est reproché à la société, en pleine guerre en Ukraine et alors que plusieurs pays mettaient en place des « *task forces* » pour identifier et geler les avoirs des oligarques russes, d'avoir laissé des proches du Kremlin déplacer d'importantes sommes d'argent via ses services[64]. Par exemple, un client de FINAPORT aurait retiré plus de 500 millions de dollars d'un compte dans une banque russe qui s'est par la suite effondrée. Aussi, un autre client aurait ouvert plusieurs comptes bancaires sous une fausse identité et y aurait transféré de l'argent malgré les inquiétudes soulevées par les personnes en charge de la conformité bancaire. FINAPORT aurait aussi travaillé avec une femme d'affaires qui s'avérait être la conjointe du dirigeant d'une entreprise publique russe ayant soutenu l'effort de guerre en Ukraine. Les griefs soulevés par les journalistes sont multiples et se basent sur la fuite de donnée succinctement servie sur un plateau d'argent par le groupe ALPHV.

---

[62] Les CONTI LEAKS ainsi que le projet RANSOMCHATS sont trés éclairant à ce sujet. Voir : https://github.com/TheParmak/conti-leaks-englished et https://github.com/Casualtek/Ransomchats

[63] Selon ses statuts disponibles ci-aprés : « European Companies Search Engine : NorthData », s. d. https://www.northdata.com/?id=6132755186.

[64] Les Echos. « Ukraine : Bercy organise la traque des biens des oligarques russes », 1 mars 2022. https://www.lesechos.fr/economie-france/budget-fiscalite/ukraine-bercy-organise-la-traque-des-biens-des-oligarques-russes-1390542.

2. Des révélations sur un géant de la télécommunication qui intéressent la justice portugaise

Le 5 septembre 2022, la rédaction du journal d'investigation REFLET.INFO débute une série de publication intitulée « *ALTICE au pays des pirates* ». Leurs enquêtes se focalisent sur le groupe français de télécommunication et plus particulièrement sur son président Patrick Drahi et son bureau de gestion de patrimoine basé en Suisse, ALTICE CAPITAL. Effectivement, un mois plus tôt, les pirates informatiques du groupe cyber rançonneurs HIVE venaient déverser sur leur site des centaines de milliers de documents internes à la société[65]. Voulant châtier publiquement la société pour ne pas avoir payé une rançon, les experts en pénétration des réseaux informatiques et en phishing du groupe HIVE ne s'attendaient sûrement pas à ce que leur méfait soit accueilli comme un véritable cadeau pour les journalistes. Il en est de même pour les pirates du groupe RANSOM HOUSE qui publièrent six mois plus tard 2,7 téraoctets de données du gouvernement de St. Kitts & Nevis (anciennement ETNC jusqu'en 2011) et dans lesquelles figurent également des informations sur le groupe ALTICE et son président, qui bénéficie de la nationalité de l'archipel. Les journalistes ont épluché ces centaines de milliers de documents afin de dresser une véritable enquête patrimoniale et financière de la société et de son président. Ainsi, les articles détaillent grâce aux factures provenant des cyberattaques, des achats de tableaux de maîtres stockés dans des ports francs, des bijoux de grande valeur ainsi que divers achats immobiliers en millions de dollars à travers le monde. Par ailleurs, les méthodes d'ingénierie fiscales et financières du groupe y sont exposées par de nombreux tableurs Excel et courriels Outlook.

Autant d'éléments matériels susceptibles de caractériser, le cas échéant, des potentielles infractions pénales[66], d'autant plus qu'une année après la publication de ces données, la justice portugaise a ouvert en juillet 2023 une enquête pour corruption et blanchiment au sujet de la filiale portugaise du groupe ALTICE et de son président, Mr Armando Pereira[67]. Les magistrats portugais suspectent Mr Pereira ainsi que plusieurs de ses proches, notamment Hernâni Vaz Antunes d'avoir imposé au fil des années des sociétés intermédiaires intercalées entre

---

[65] Le groupe HIVE a été démantelé lors d'une opération commune entre le FBI et EUROPOL. Le site internet hébergé sur le réseau TOR n'est donc plus disponible.

[66] À ce stade, toute personne reste présumée innocente.

[67] Queirós, Óscar. « Armando Pereira e Vaz Antunes presos em casa sem pagar caução ». Jornal de Notícias (blog), 24 juillet 2023. https://www.jn.pt/7993107800/armando-pereira-e-vaz-antunes-presos-em-casa-sem-pagar-caucao/.

ALTICE et ses fournisseurs habituels en matière de télécommunications[68]. Ces derniers devaient traiter avec des sociétés telles que INTECIAL, JANA GENERAL TRADINF ou ACIERNET pour fournir le groupe. Toutes ces sociétés intermédiaires s'avèrent, *in fine*, bénéficier aux comparses suspectés d'avoir ourdi le stratagème.

Là encore les journalistes de STREET PRESS et BLAST, Antoine Champagne, Clara Monnoyeur et Mathieu Molard, ont passé au tamis les documents publiés par les groupes HIVE et RANSOM HOUSE au travers de ce qu'ils nomment sous un même sobriquet les « *Drahi Leaks* ».

Ces documents apportent, selon leurs déclarations, des éléments susceptibles d'entrer en résonance avec l'affaire judiciaire au Portugal et sur la responsabilité du président directeur général du groupe. Les journalistes précisent dans leurs articles : « *Les **DrahiLeaks** montrent qu'au sein d'Altice 11 personnes à peine, dont Armando Pereira, contrôlent toutes les entités et prennent toutes les décisions importantes. Rien ne leur échappe.* »

—

« *Les **DrahiLeaks** démontrent qu'une partie des sociétés considérées par la justice portugaise comme participant du système de parasitage d'Altice par Armando Pereira sont en fait des sociétés créées et contrôlées par Altice. Prenons Intelcia, selon les enquêteurs portugais, ce prestataire aurait généré des commissions indues en facturant Meo, l'une des marques d'Altice Portugal. Or Intelcia n'est en rien indépendante, c'est Patrick Drahi qui en contrôle la destinée, comme nous l'avions raconté ici. Il l'utilise notamment pour externaliser et délocaliser (au Maroc) ses services clients*. »

—

« *Le pool des **DrahiLeaks** a déniché un autre document en lien avec une opération elle aussi jugée frauduleuse par la justice : "l'Audit Commitee" toujours évoqué au détour de l'un de ses rapports le montage financier qui entoure la vente de biens immobiliers d'Altice Portugal à Almost Future, une autre entité gérée par Hernâni Vaz Antunes. Les inspecteurs d'Altice ne trouvent absolument rien à redire à l'opération en cours, notant juste qu'elle n'apparaît pas encore dans le bilan comptable. La justice portugaise va découvrir qu'Hernâni Vaz Antunes a réalisé un tour de passe-passe sur cette opération immobilière, pour encaisser plusieurs millions d'euros en revendant les immeubles avant d'avoir fini de les payer à Altice Portugal.* »

---

[68] Também, Leia. « Altice aceitou proposta de Vaz Antunes após recusar uma mais alta ». Jornal de Negócios (blog), s. d. https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/venda-de-data-centers-pode-render-700-milhoes-a-altice.

Sérgio Azenha, António, et Tânia Laranjo. « Milionário da Altice ganha 32 milhões de euros em esquema suspeito ». Correio da Manhã (blog), 24 juillet 2023. https://www.cmjornal.pt/portugal/detalhe/milionario-da-altice-ganha-32-milhoes-de-euros-em-esquema-suspeito.

À l'image des articles sur GENESIS TRUST & CORPORATE SERVICES, une grande partie des informations provenant de rançongiciels à double extorsion ont servie de base à l'enquête des journalistes.

B. Un processus d'identification et de veille facilement reproductible

Afin de déterminer le potentiel de ces données dans le cadre d'enquêtes financières et patrimoniales, la section ci-après s'inscrit dans une démarche pratique. Cette dernière reflète la vocation du master IFEE quant à la conjugaison de connaissances en droit pénal des affaires et de méthodes d'investigation. La première partie exposera une méthodologie permettant d'identifier des éléments d'intérêt suite à des attaques aux rançongiciels par double extorsion. La seconde quant à elle décrira plus amplement les informations collectées au cours de cet essai et leurs liens avec des thématiques liées à l'investigation financière.

1. L'identification de la donnée d'intérêt

Deux axes de recherches peuvent être développés, un géographique et un autre par entités. Premièrement, il est possible de constater que de nombreux groupes d'attaquants publient le nom de leurs victimes en indiquant leur site internet via leur nom de domaine (Domain Name Server en anglais abrégé en DNS) ainsi que leur extension (Top-Lever Domain). L'internet Assigned Numbers Authority (IANA) recense plusieurs milliers de TLD qui peuvent être choisi librement par toute personne souhaitant créer un site internet. Des TLD géographiques, comme « . vg », existent et peuvent s'avérer utiles pour identifier une société basée dans un ETNC, notamment des sociétés fiduciaires. En illustre l'exemple de GENESIS TRUST & CORPORATE SERVICES qui disposait d'un site internet[69] en « .ky », signifiant un rattachement aux îles Cayman. Suivant cette logique il est possible de lister les 23 TLD rattachés à des ETNC selon la liste de l'UE des pays et territoires non coopératifs à des fins fiscales du 17 octobre 2023.

Pays / Territoire	Pays qui coopèrent avec l'UE et n'ont pas d'engagements en cours de mise en œuvre	Pays qui ne coopèrent pas avec l'UE ou n'ont pas pleinement mis en œuvre leurs engagements	Pays qui coopèrent avec l'UE et ont des engagements en cours de mise en œuvre	TLD associé
Anguilla		X		.ai

[69] *genesis.ky archivé sur : https://web.archive.org/web/20210419044016/https://www.genesis.ky/*

Pays / Territoire	Pays qui coopèrent avec l'UE et n'ont pas d'engagements en cours de mise en œuvre	Pays qui ne coopèrent pas avec l'UE ou n'ont pas pleinement mis en œuvre leurs engagements	Pays qui coopèrent avec l'UE et ont des engagements en cours de mise en œuvre	TLD associé
Antigua-et-Barbuda		X		.ag
Bahamas		X		.bs
Belize		X		.bz
Bermudes			X	.bm
Guam		X		.gu
Guernesey			X	.gg
Îles Féroé			X	.fo
Îles Marshall				.mh
Île de Man			X	.im
Iles Caymans	X			.ky
Îles Cook			X	.ck
Îles Turques et Caïques		X		.tc
Îles Vierges britanniques			X	.vg
Jersey			X	.je
Liechtenstein			X	.li
Panama		X		.pa
Saint-Vincent-et-les-Grenadines			X	.vc
Samoa		X		.ws
Samoa américaines		X		.as
Seychelles		X		.sc
Trinité-et-Tobago		X		.tt

Pays / Territoire	Pays qui coopèrent avec l'UE et n'ont pas d'engagements en cours de mise en œuvre	Pays qui ne coopèrent pas avec l'UE ou n'ont pas pleinement mis en œuvre leurs engagements	Pays qui coopèrent avec l'UE et ont des engagements en cours de mise en œuvre	TLD associé
Vanuatu		X		.vu

(Tableau réalisé par l'auteur de ce mémoire)

La deuxième logique se base sur les OFFSHORE LEAKS publiées par l'ICIJ et qui rassemblent la totalité des personnes morales (PM) présentes dans les fuites de données étudiées par le consortium[70] et les données d'OPEN SANCTION[71] qui regroupent l'ensemble des PM mises sous sanctions internationales par différents gouvernements[72].

Regroupant plus de 810 000 PM pour les OFFSHORE LEAKS et 401 698 PM pour la liste OPEN SANCTION, ces deux sources de données ont l'avantage d'être disponibles au format CSV permettant un croisement et un travail facile sous forme de tableur via MICROSOFT EXCEL ou LIBRE OFFICE CALC. Une troisième méthode consiste quant à elle à rechercher des entreprises via des mots clés souvent utilisés pas les entreprises fiduciaires ou *offshore* (*trust, trustee, shell company,* etc..) ou par le nom de certaines entreprises d'intérêt (Henley & Partners, ou Studhalter International Group AG par exemple).

2. Une exhumation de cas intéressants

L'entreprise américaine Microsoft Threat Intelligence dénombrait plus de 100 groupes cybercriminels mettant en œuvre des rançongiciels. La quasi-totalité de ces groupes dispose de leur propre site en .onion (*hidden service*) accessible via TOR. Afin d'accéder à l'historique des publications de ces sites en un seul lieu, il

[70] La base de donnée « OFFSHORE LEAKS » regroupé la totalité des entités nommées présentes dans les Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers et les Offshore leaks. Voir https://offshoreleaks.icij.org/pages/database

[71] Projet crée et maintenue par la société allemande OpenSanctions Datenbanken GmbH.

[72] 87 programmes de sanctions sont actualisé et mis à disposition par OPEN SANCTION. La liste des programme sur lesquels se base la société pour mettre à disposition sa liste consolidée est disponible à l'adresse suivante : https://www.opensanctions.org/datasets/default/

est possible d'utiliser le site *ransomware.live*[73], dérivé du projet *ransomwatch*[74]. Il est possible d'extraire un fichier .csv de l'ensemble des victimes touchées, (9525 en décembre 2023) par plus de 150 groupes cyber criminels.

Le croisement de ces données permet d'obtenir des résultats intéressants et d'identifier 10 sociétés victimes de rançongiciels impliqués dans les « offshore leaks », mises sous sanction ou proposant des services fiduciaires dans des ETNC. Les données internes de ces 11 entreprises ont été diffusées sur les sites des attaquants.

Victime	Présente dans	Ransomware	Date
Cromwell Management Inc.	Offshore leaks	Karakurt	11/12/2022
DCI, Inc.	Offshore leaks	Conti	23/10/2021
Dynamite	Offshore leaks	Stormous	24/07/2023
El Milagro	Offshore leaks	Akira	24/07/2023
Equadore Trustee	Mots clés	LockBit	16/09/2022
Genesis Trust And Corporate Services ltd	TLD d'ETNC	LockBit	18/03/2022
Gleason Corporation	Offshore leaks	Conti	04/05/2022
Jammal Trust Bank	Sanctions	Vice Society	23/08/2022
Ocean	Offshore leaks	Stormous	23/05/2023
The Beacon Insurance Company Limited	Offshore leaks	Dataleak	11/12/2022
UMV Group	Offshore leaks	Ransomexx	10/12/2021

(Tableau réalisé par l'auteur de ce mémoire)

Conclusion du chapitre I

L'explosion du nombre d'attaques aux rançonlogiciels, et donc du nombre de victimes touchées, a statistiquement induit que des entreprises s'adonnant à des délits ou des fraudes soient touchées. Parallèlement, le modèle de chantage des groupes cybercriminels a évolué vers une publication complète des données exfiltrées en cas de non paiement des rançons. Disséminées sous la forme d'archives de plusieurs centaines de gigaoctets, majoritairement à travers les « *hidden-servicies* » du réseau TOR, elles ont suscité l'intérêt des curieux, des

[73] https://www.ransomware.live/#/allvictims

[74] https://ransomwatch.telemetry.ltd/#/

experts en cybersécurité, des concurrents de ces victimes, ainsi que d'autres cybercriminels avides de données (documents d'identités, couple login/mot de passe) pour prévoir leurs futurs méfaits. Plus récemment, ces données sont rentrées dans le radar des journalistes d'investigations qui s'en sont emparés pour exposer au travers d'enquêtes ce qu'ils présentent être des infractions financières ou fiscales.

Ainsi, au moins trois cas, traités par des journaux suisses et français, reposant exclusivement sur ce vecteur ont été identifiés. Également, via une méthodologie développée dans ce chapitre, dix entreprises en lien avec l'évasion fiscale ou sous sanction internationale et ayant vu leurs données internes diffusées à la suite d'une attaque aux rançongiciels ont été détectées.

Bien que l'utilisation de ces données dans le cadre d'enquêtes soit récente, le premier cas recensé datant d'avril 2022, il est probable que ce type de données soient utilisées plus amplement à l'avenir, notamment par les journalistes.

CHAPITRE II : Son utilisation dans un cadre judiciaire

Selon le Conseil de l'Europe et le groupe d'action financière (GAFI), l'investigation financière peut mobiliser certaines « *techniques spéciales d'investigation* »[75] souvent qualifiés « *d'intrusives et aboutissent à l'obtention d'informations privées sur un individu* »[76]. En France, le Code de procédure pénal (CPP) permet aux magistrats d'obtenir des copies complètes de supports numériques (serveurs, disques de stockage) au cours de perquisitions. Qualifiés de « télé perquisitions » par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)[77], ce dispositif peut être mis en œuvre lors de flagrants délits selon l'article 56 du CPP, lors d'enquêtes préliminaires conformément l'article 76 et également lors de commissions rogatoires en accord avec l'article 97-1. Plus encore les magistrats peuvent recourir lors de procédures judiciaires, à distance et sans le consentement

[75] *GAFI. « Operational Issues - Financial Investigations Guidance », juin 2022. Page 6 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf.*

[76] *Ibid p.7*

[77] *NAEL, Olivier. « La "télé" perquisition - OCLCTIC ». s. d. https://clusif.fr/wp-content/uploads/2015/09/clusif-forensics-2010-teleperquisition-oclctic.pdf.*

des intéressés, à des actions de recueil de données informatiques[78] (RDI, pour le stock) et à des captation de données informatiques (CDI, pour le flux) par l'intermédiaire du discret Service technique national de captation judiciaire[79] (STNCJ). Un article publié par Matthieu Audibert dans la revue *Archives de politique criminelle,* détaille le fonctionnement et l'encadrement juridique de tels outils dans le cadre de procédures judiciaires[80].

« *La loi du 23 mars 2019 est venue réorganiser les dispositions relatives à l'encadrement des techniques spéciales d'enquête. Ainsi, la captation des données informatiques est limitée aux d'infractions d'une "particulière gravité et complexité" qui doivent nécessairement entrer dans le champ d'application des articles 706-73 et 706-73-1 du code de procédure pénale et si les nécessités de l'enquête ou de l'information l'exigent. Autrement dit, il faut préalablement justifier dans la procédure la nécessité de recourir à cette technique spéciale d'enquête avant de solliciter toute demande d'autorisation. Cette autorisation est obligatoirement délivrée par un magistrat du siège : dans le cadre de l'enquête, par le juge des libertés et de la détention à la requête du procureur de la République, dans le cadre de l'information, par le juge d'instruction, après avis du procureur de la République. Ensuite le juge doit impérativement rendre une ordonnance écrite et motivée comportant des éléments de fait et de droit pour justifier que cette opération est nécessaire* ».

Le Conseil constitutionnel l'a rappelé en 2019[81], ces procédures doivent être réservées aux affaires les plus graves qui concernent, entre autres, les délits de blanchiment d'argent résultant des 12 infractions[82]. Il est donc possible pour un service d'enquête financier de recourir à des « t*echniques spéciales*

---

[78] RDI : Afin de récupérer les données enregistrés sur un support
CDI : Notamment pour obtenir l'information tel qu'affichée à l'écran .
A ce sujet voir notamment : le rapport d'information déposé par la mission d'information commune, sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement. https://www.assemblee-nationale.fr/dyn/docs/RINFANR5L15B3069.raw et l'article https://www.intelligenceonline.fr/renseignement-d-etat/2022/02/18/l-enquete-par-infiltration-numerique-encrochat-attaquee-en-justice-de-toutes-parts,109734739-art

[79] Crée en 2018, le STNCJ est administrativement rattaché à la DGSI. Voir : Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire », INTR1802937A § (2018). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036887904.

[80] Audibert, Matthieu. « La pénétration du droit pénal dans l'espace privé. La captation de données informatiques », Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 91-103.

[81] Conseil constit. 21 mars 2019, n°2019-778 DC, §162: https://www.conseil-constitutionnel.fr/decision/2019/2019778DC.htm

[82] Issues des articles 706-73 et 706-73-1 du Code de procédure pénale

d'investigations », selon la qualification du GAFI, de même qu'a des dispositifs légaux intrusifs.

Plusieurs questions se posent dès lors. Que ce passe-t-il si, à la suite d'une perquisition et d'une copie des supports numériques (ordinateurs/serveurs) d'une entreprise réalisée dans le cadre affaire financière, il s'avère que ces données sont beaucoup moins riches en informations que celles publiées quelques mois plus tôt par des cyber rançonneurs ? Plus encore, si de telles copies ne peuvent pas être réalisées, car l'entreprise se situe dans un ETNC, des services axés sur les infractions financières ou fiscales (DNEF, DNRED, OCLIF, SNDJ, BRIF etc..) peuvent-ils se saisir de ces données ? Quels seraient leur statut ainsi que leur recevabilité ?

L'exemple des « *DrahiLeaks* » reflète bien cette problématique. Les documents concernant Armando Pereira, diffusés par HIVE et RANSOM-HOUSE et mis en relief par les journalistes français, peuvent-ils être utilisés ? Ainsi, le deuxième chapitre de ce mémoire se focalisera sur les notions juridiques sous-jacentes ainsi que sur la jurisprudence en vigueur sur le sujet.

Section 1. Les fuites de données au regard de la loi

Après avoir étudié les mécanismes et les tendances des attaques aux rançongiciels ainsi que l'apport latent des données exfiltrées au cours de ces attaques dans des investigations, il convient désormais de décortiquer ce sujet par le prisme du droit. Plus précisément, la première section de ce chapitre aura pour but de préciser les différentes catégories de fuite de données ainsi que les infractions qui peuvent s'y rattacher, en particulier pour les fuites indues d'attaques aux rançongiciels, avant d'analyser les conditions d'apport de la preuve en matière de droit pénal.

§1. Les enjeux connexes

Le CNRTL définit la fuite comme « la *mise à jour, divulgation de documents qui auraient dû rester secrets* »[83], sa traduction en langue anglaise, « *leak* », donne une définition similaire selon l'OXFORD DICTIONARY « *to give secret information to the public* »[84]. Partant de ce postulat, l'utilisation de ces informations s'avère délicat. Cependant, qu'entend-on réellement par « fuite de

[83] *CNRTL. « Définition du mot "fuite" ». Centre national de ressources textuelles et lexicales (blog), https://www.cnrtl.fr/definition/fuite.*

[84] *Cambridge Dictionary. « Leak defintion », s. d. https://dictionary.cambridge.org/fr/dictionnaire/anglais-francais/leak.*

donnée » ou « *leaks* » ? Leur utilisation relève t-elle systématiquement de l'infraction ?

A. Fuite de donnée : un terme polysémique

1. Une expression polysémique impliquant des notions de droit distinctes

Les différents médias en ligne ainsi que les principaux quotidiens nationaux français ont largement utilisé le terme de « fuite de données » ou « *leaks* » pour désigner, de manière générale, la divulgation à des tiers d'informations présentes dans des systèmes informatiques. Il est possible de constater qu'il n'existe pas, en droit français de même que dans l'usage courant, de définition stricte d'une fuite de donnée.

Pourtant, des nuances existent en particulier sur la manière dont ces dernières peuvent avoir lieu et leurs accès par des tiers. Il est possible de distinguer quatre grandes catégories de « fuites de données » ayant leurs propres logiques et faisant appel à des notions juridiques différentes. Le tableur réalisé ci-dessous tente d'en définir les contours.

CATEGORIE DE FUITES DE DONNES					
Nom détaillé	**Cause de la fuite de donnée**	**Spécificité**	**Intention de l'auteur**	**Exemples**	**Librement accésible**
Fuite de donnée involontaire	Mauvaise configuration informatique	La personne à l'origine de la fuite n'a pas conscience de divulguer de l'information	Aucune	RIFI/DFIR, affaire « Bluetouff »	Oui
Fuite de donnée d'informateurs	Lanceurs d'alerte	Souvent délivrées à destination des journalistes, les données brutes ne sont pas accessibles	Motivation idéologique	PANAMA PAPERS; DUBAI UNCOVERED	Non
Fuite de donnée par des cyber acteurs malveillants (*Intelligence broker)*	Piratage	Données payantes	Générer un profit	RAID FORUM, BREACH FORUM	Partiellement

CATEGORIE DE FUITES DE DONNES					
Nom détaillé	**Cause de la fuite de donnée**	**Spécificité**	**Intention de l'auteur**	**Exemples**	**Librement accésible**
Fuite de donnée par double extorsion	Piratage par rançongiciels	Accessible par tous via les « *hidden services* » du réseau TOR.	Dissuader les prochaines victimes	FINAPORT LEAKS, DRAHI LEAKS	Oui

(Classification réalisée par l'auteur de ce mémoire)

Comme le précise bien Lindsay Freeman dans son article intitulé « *Hacked and leaked: legal issues arising from the use of unlawfully obtained digital evidence in international criminal cases* », une différence stricte doit être opéré entre les donnée piratées et celles divulguées : « *for clarity, hacked information is information acquired by an out- sider who gains unauthorized access to it, whereas leaked information is information obtained by an insider who has authorized access to it, but shares it in an unauthorized manner.* »[85].

2. Le cas particulier des fuites de données issues de rançongiciels

Les fuites de données issues d'attaques aux rançongiciels ainsi que leur spécificité, constituent le cœur de la réflexion de ce mémoire. Pour ce type de fuite, à l'inverse des données provenant de lanceurs d'alerte ou d'une mauvaise configuration informatique, une attaque informatique a été perpétrée sur les systèmes informatiques d'une société. De plus, la diffusion de ces données ne constitue pas la motivation première des cyber rançonneurs. Contrairement aux données extirpées par des cyber acteurs malveillants qui réalisent ces attaques pour vendre ou échanger ces données, celles provenant des rançongiciels sont mises à disposition librement à toute personne[86].

B. Les infractions associées aux attaques par rançongiciels

Trois infractions peuvent être identifiées au sujet des attaques par rançongiciels. Plus précisément, il s'agit respectivement d'une atteinte aux systèmes de traitement automatisé de donnée au sens de l'article 323-3 du CP et d'un délit de recel selon l'article 321-1. L'analyse juridique de ces infractions permettra d'apprécier au mieux la réponse concernant l'exploitation de ces données.

---

[85] *Traduction du rédacteur : « Pour plus de précision, une information piratée correspond à une information acquise par une personne extérieure qui y accède sans autorisation, tandis qu'une information divulguée correspond à une information obtenue par un individu qui y accède de manière autorisé de l'intérieur, mais qui la partage de manière non autorisée. »*

[86] *Fuite de donnée par courtiers en renseignements (Intelligence broker) selon la qualification de ce mémoire.*

1. L'atteinte aux systèmes de traitement automatisé de donnée (STAD)

L'atteinte au STAD est un délit défini aux articles 323-1 à 323-8 du CP français. Il convient de préciser que la notion de STAD a été introduite en droit français par la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique (dite loi Godfrain). Les STAD n'ont pas été définis strictement afin de ne pas subir les différentes évolutions technologiques. La jurisprudence française propose ainsi une conception élargie de la notion de STAD, allant par exemple du support numérique tel qu'un disque dur (Cour d'appel de Douai, 7 oct. 1992), au serveurs informatique d'une société (Cour de cassation, Chambre criminelle, 20 mai 2015) en passant par le réseau carte bancaire (Trib. cor. Paris, 25 fev. 2000).

Les actes punis par les articles 321-1 à 321-4 sont variés. Ces dispositions embrassent tous les actes depuis la préparation jusqu'à sa matérialisation, en comprenant également leur tentative :

- l'accès ou le maintien frauduleux dans un système de traitement automatisé de données (article. 323-1, al. 1er du CP), avec une circonstance aggravante en cas de suppression ou de modification des données contenues dans le système ou son altération du fonctionnement (article 323-1, al. 2 du CP). Peine encourue : 3 ans de prison et 100 000 € d'amende ;

- le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données (article 323-2 du CP). Peine encourue : 5 ans de prison et de 150 000 € d'amende ;

- le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier les données (article 323-3 du CP). Peine encourue : 5 ans de prison et de 150 000 € d'amende ;

- l'importation, la détention, l'offre, la cession ou la mise à disposition d'équipement, d'instrument, de programme informatique ou tout donné conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 (article 323-3-1 du CP). Peine encourue : 5 ans de prison et de 150 000 euros d'amende. ;

- la participation à un groupe formé ou à une entente établie en vue de commettre des fraudes informatiques (article 323-4 du CP). Peines encourues : similaire que l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Si ces actes ont été commis à l'encontre d'un STAD mis en œuvre par l'État, la peine encourue est portée à sept ans de prison et à 300 000 € d'amende. Si ces actes ont été commis en bande organisée, la peine est portée à dix ans de prison et 300 000 € d'amende. Au niveau européen une directive passée en août 2013 prévoit l'harmonisation de la législation des États membres en matière d'attaques contre les systèmes d'information et l'extension des infractions qui s'y rapportent[87].

Les attaques aux rançongiciels touchant en trés grande majorité des entreprises, il convient de mentionner que la violation du secret des affaires ne s'applique pas en matière de droit pénal. De même, la violation du secret de fabrique ou celle du secret professionnel ne s'applique qu'aux salariés ou directeurs d'une entreprise[88]. En tout étant de cause, la loi du 30 juillet 2018[89] a prévu des dérogations au secret des affaires pour permettre de garantir l'exercice des pouvoirs d'enquête, de contrôle, des autorités juridictionnelles ou administratives[90]. Les attaques aux rançongiciels, en copiant les données présentes sur les systèmes informatiques d'une entreprise et en chiffrant ces dernières, répondent bien à l'infraction d'atteinte au SATD au sens de l'article 323-3 du CP qui sanctionne « *le fait d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier les données* ».

2. L'extorsion

L'extorsion est un délit défini aux articles 312-1 à 312-9 du CP français qui visent à sanctionner le fait d'obtenir par violence, menace de violence ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque[91]. L'extorsion est punie de 7 ans de prison et de 100 000 euros d'amende. Les cyber attaquants utilisant des rançongiciels, en contraignant leurs victimes par la privation de leurs données au moyen du chiffrement informatique, et en leur fournissant la clé de déchiffrement en échange d'un paiement d'une rançon, se rendent effectivement coupables d'une extorsion selon la loi française.

---

[87] *Parlement Européen. DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, Pub. L. No. 12 aout 2013, L 218/8 (s. d.). https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32013L0040&from=SL.*

[88] *Commission d'accès aux documents administratifs. « Les secrets protégés par la loi », s. d. https://www.cada.fr/particulier/les-secrets-proteges-par-la-loi.*

[89] *LOI n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires*

[90] *Article L151-7 du Code de commerce :* https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266571/2018-08-01

[91] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418160

(Extrait d'une conversation entre le groupe LOCKBIT 3.0. et une de ses victimes. Les messages font clairement état de menaces quant au déchiffrement des données et la publication de ces derniers en cas de non-paiement de la rançon [92]. Source : https://ransomch.at/lockbit3.0-**********149576)

[92] *Traduction du rédacteur : « LOCKBIT 3.0 : Gardez bien à l'esprit que nous avons volés toutes vos données et que nous pouvons les publier à tout moment. Nous vous proposons de déchiffrer tout vos fichiers ainsi que votre HYPERVISOR pour 1 millions de $ »*

3. Le recel

Les données publiées à la suite d'une attaque aux rançongiciels sont donc intimement liées à deux infractions, l'atteinte aux STAD (article 323-3 du CP) et l'extorsion (articles 312-1 du CP). Par conséquent l'utilisation de ces données s'avère épineuse en vertu du délit de recel défini aux articles 321-1 à 321-5 du CP. Le recel est une infraction de conséquence qui consiste à réaliser intentionnellement certains actes sur une chose que l'on sait provenir d'un crime ou d'un délit. Ces agissements sont punis de 5 ans de prison et de 375 000 euros d'amende.

Plus précisément, l'article 321-1 du CP sanctionne le fait de « *dissimuler, de détenir ou de transmettre une chose (...) en sachant que cette chose provient d'un crime ou d'un délit.* » Constitue également un recel *"le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit"*. » La chose recelée peut être un bien matériel (bijoux, documents) autant qu'un bien immatériel (abus de faiblesse, trafic d'influence).

Ainsi, deux catégories de recels peuvent être distinguées. Premièrement, le « recel maîtrise »[93] qui concerne ceux qui détiennent la chose provenant d'un délit ou d'un crime, mais également les intermédiaires qui en amont l'ont dissimulée, ou transmise pour le bénéficiaire ultime. Deuxièmement, le « recel profit »[94] vise quant à lui les personnes qui bénéficient, par tout moyen, du produit d'un délit ou d'un crime si elles ont connaissance de son origine illégale. La référence au « produit », qui transcende donc l'objet du délit ou du crime, permet à la chambre de cassation de juger que le recel concerne également les choses qui lui sont substituées (duplication par exemple)[95]. La Cour de cassation juge cependant que la bonne foi d'une personne lors de son entrée en possession avec la chose recelée donc à son insu, permet d'écarter la caractérisation du recel (Cour de Cass, Chambre crim, 24 janvier 1978).

Dans le cadre des fuites de données aux rançongiciels, l'utilisation de ces documents pourrait être qualifiée pénalement de recel d'atteintes aux systèmes de traitement automatisé de données (STAD) ou de recel d'extorsions.

§2. La recevabilité de la preuve

---

[93] *Dreyer, Emmanuel. « Chapitre 1. Le recel du produit des atteintes aux biens », , Droit pénal spécial. sous la direction de Dreyer Emmanuel. Ellipses, 2016, pp. 565-580.* https://www.cairn.info/droit-penal-special--9782340014015-page-565.htm

[94] *ibid*

[95] *ibid*

Les données issues d'attaques aux rançongiciels, bien que publiques, sont inhérentes aux infractions d'atteinte aux STAD (art 323-3 du Code pénal) et d'extorsion (art 312-1 du Code pénal). Cependant, est-il possible par un effet miroir d'exposer un délit par un acte illégitime lors d'une enquête ? Des principes spécifiques existent en droit français au sujet de l'apport de la preuve (A) de même que des statuts particuliers permettent certaines protections (B).

A. La légalité et la loyauté de la preuve en France

1. Mécanisme dans le cadre d'affaires civiles

Pour les affaires civiles, la preuve doit être légale (C.pr.civ, art 9) et soumise aux règles du contradictoire (C.pr.civ, art 16). Un principe de loyauté, qui vise à respecter les droits des individus, s'y applique également bien qu'il ne soit établi formellement dans le Code de procédure civil. Ce principe de loyauté constitue néanmoins un objectif premier pour les juges civils qui lui accorde une place importante depuis de nombreuses années au titre de l'équité des procès[96] en ce référent notamment au premier paragraphe de l'article 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et le principe de loyauté dans l'administration de la preuve du Conseil de l'Europe[97]. La Cour de cassation, constituée en assemblée plénière, l'a rappelé en 2011 dans un arrêt [98]:
« *est irrecevable à titre de preuve devant le Conseil de la concurrence[99] Un enregistrement obtenu à l'insu d'une personne, en contravention avec le principe de loyauté qui doit présider à l'obtention des preuves ; qu'en décidant le contraire, la Cour d'appel a violé les textes susvisés et le principe de loyauté en matière d'obtention des preuves* ».

2. Mécanisme dans le cadre d'affaires pénales

Le Code de procédure pénal a sa propre logique, notamment via son article 427 qui indique : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime*

---

[96] Touret, Franck. « Corrigé Droit civil ENM 2017 : La loyauté de la preuve dans le procès civil », 2017. https://www.prepa-isp.fr/wp-content/uploads/2018/09/ENM-Annales-Civil-2017.pdf.

[97] Conseil de l'Europe. Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales telle qu'amendée par les Protocoles n° 11 et n° 14 (1950).

[98] Cour de cassation, Assemblée plénière, 7 janvier 2011

[99] Sauf disposition contraire du Code de commerce, les règles du Code de procédure civile s'appliquent aux contentieux anticoncurrentielles relevant de l'Autorité de la concurrence.

conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui ».

La preuve peut donc être administrée par la partie poursuivante de manière beaucoup plus large qu'au civil tant que cette dernière est portée à la connaissance des parties et soumise aux débats[100]. Elle est donc prise avant tout pour sa valeur et non son origine. Un arrêt de la Cour de cassation (Cour de Cass, Chambre crim, 11 juin 2002) illustre ce mécanisme.

L'association SOS RACISME avait réalisé des enregistrements clandestins afin de montrer que certaines entreprises s'adonnaient à de la discrimination[101]. La chambre criminelle, bien que rejetant l'infraction de discrimination, a reçu les enregistrements comme une preuve « ordinaire »[102] et a déclaré dans son jugement « *Aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale. Il leur appartient seulement, en application de l'article 427 du Code de procédure pénale, d'en apprécier la valeur probante* ». La preuve peut donc être illicite et déloyale lorsqu'elle est présentée par des parties privées.

B. Une latitude dans l'apport de la preuve pénale différente pour les parties publiques

1. Le recueil par stratagèmes : entre constatation et incitation, la recevabilité en est viciée

Concernant les parties publiques, elles doivent se borner à la légalité de la preuve ainsi qu'au principe de loyauté lors des recueils effectués. En effet, une provocation visant à constater et caractériser l'infraction qui en découle pour mieux condamner ensuite, est proscrit. Les magistrats de la Cour de cassation l'on rappelé en 2015 (Cour de cass, Assemblée plénière, 6 mars 2015) « *porte atteinte au droit à un procès équitable et au principe de loyauté des preuves le stratagème qui en vicie la recherche par un agent de l'autorité publique* ».

Que faire cependant lorsque que des infractions sont si difficiles à caractériser qu'elles nécessitent d'y participer indirectement, c'est-à-dire sans aucune provocation ni incitation, afin de constater le méfait. En miroir de la provocation à l'infraction, attentatoire à un procès équitable, se trouve ainsi la provocation à

---

[100] *Rellé, Aaron. « Le droit de la preuve en matière pénale ». VILLAGE DE LA JUSTICE (blog), 17 mai 2023. https://www.village-justice.com/articles/droit-preuve-matiere-penale,45864.html.*

[101] *Beroule, Marie. « La loyauté de la preuve pénale ». Mémoire de recherche, AIX-MARSEILLE UNIVERSITE FACULTE DE DROIT ET DE SCIENCE POLITIQUE, 2022. P 29 https:// dumas.ccsd.cnrs.fr/dumas-03541064/document.*

[102] *Ibid*

la preuve[103], notion qui permet effectivement la constatation d'une infraction préalablement existante en respectant les droits fondamentaux. Les magistrats de la Cour de cassation désignent ces actions par le mot « stratagème » dans leurs délibérations. Récemment, la Cour de cassation (court de Cass, Assemblée plén, 9 décembre 2019) a considéré comme recevables les éléments issus de l'infiltration d'un policier dans une affaire de chantage : « *Le stratagème employé par un agent de l'autorité publique pour la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas en soi une atteinte au principe de loyauté de la preuve. Seul est proscrit le stratagème qui, par un contournement ou un détournement d'une règle de procédure, a pour objet ou pour effet de vicier la recherche de la preuve en portant atteinte à l'un des droits essentiels ou à l'une des garanties fondamentales de la personne suspectée ou poursuivie.* »[104] Ces stratagèmes sont acceptés de manière assez large, un arrêt de la Cours de cassation (Cour de cass, Chambre crim, 30 avril 2014) juge en effet recevables les éléments issus d'un forum de discussion en ligne frauduleuse, crée spécifiquement par le Federal Bureau of Investigation (FBI) afin de récupérer des données de connexions (Cours de cass, Chambre crim, 30 avril 2014). Ces informations techniques avaient été transmises aux autorités françaises qui s'en étaient servie pour diligenter des perquisitions et arrêter un suspect.

Comme l'explique Marie Beroule, il est donc possible de distinguer deux types de stratagèmes dans le recueil de la preuve par l'autorité publique, l'un actif qui corrompt la procédure, l'autre passif tout à fait recevable[105].

2. Le recueil réalisé par des tiers

Une troisième catégorie peut également être remarquée : le recueil par apport externe. Ce dernier se matérialise lorsque l'autorité publique s'appuie sur des éléments dont l'origine est inconnue, mais qu'elle n'a pas collectés elle même. Ces éléments peuvent donc avoir été recueillis de façon illégale et déloyale. À ce sujet la jurisprudence (cour de Cass, Chambre crim, 1er décembre 2020) avance que le fait de ne pas pouvoir établir l'origine d'une preuve, si des vérifications pour tenter d'en connaître l'origine ont été menées, n'entrave pas sa recevabilité.

---

[103] Renucci, Jean-François. « Droits de l'homme », Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2014, pp. 843-847. https://doi.org/10.3917/rsc.1404.0843.

[104] Hervieu, Merryl. « Policier infiltré : tant qu'il n'est pas pousse au crime, le stratagème n'attente pas à la loyauté de la preuve ». DALLOZ (blog), 20 janvier 2020. https://actu.dalloz-etudiant.fr/a-la-une/article/policier-infiltre-tant-quil-nest-pas-pousse-au-crime-le-stratageme-nattente-pas-a-la/h/16019c32d59c4e5bed99f609ca39d4c2.html.

[105] BEROUL, op.cit p 56

Cette dernière avait été saisie après que des enregistrements audio diffusés par des journalistes et remis à la police avaient été utilisés lors d'une procédure[106].
L'appelant supputait que les enregistrements avaient été réalisés par l'autorité publique de manière irrégulière[107]. Les enquêtes pour déterminer l'origine des enregistrements se sont heurtées au secret des sources des journalistes laissant ainsi planer l'incertitude quant à sa filiation.

Le secret des sources des journalistes est strictement encadré en France par la loi du 4 janvier 2010 et plusieurs jurisprudences européennes l'on rappelé (CEDH 27 mars 1996, Goodwin c/ Royaume-Uni[108], CEDH 28 juin 2012, Ressiot et a. c/ France). D'une certaine manière, comme l'a montré la Cour de cassation dans son arrêt du 1er décembre 2020, le fait que cet élément soit passé dans les mains de journalistes l'a en quelque sorte blanchi.

Lors de procédures pénales il est donc possible pour l'autorité publique, par des stratagèmes passifs dans le recueil de la preuve ou par l'implication de tiers, d'utiliser des éléments déloyaux ou ayant une origine incertaine, donc potentiellement illégal.

Section 2. La réutilisation de fuite de données

Après avoir étudié le sous-jacent délictuel des attaques aux rançongiciels, la possibilité offerte par le Code de procédure pénal permettant d'accueillir la preuve de manière plus large que pour les affaires civiles ainsi que la jurisprudence en vigueur au sujet de la loyauté de la preuve, il est opportun de se questionner sur l'utilisation de fuites de données dans des procédures (1), avant de s'intéresser à celles issues spécifiquement d'attaques aux rançongiciels (2). L'étude de la jurisprudence impliquant des fuites de données de catégories différentes comme vecteur de preuve permettra de dégager une appréciation globale quant à leur recevabilité[109]. Des parallèles ou des oppositions pourront ainsi s'en dégager.

---

[106] Lavric, Sabrina. « Affaire Benalla. Preuve pénale : n'est pas irrégulière la preuve dont les conditions de recueil sont restées incertaines ». DALLOZ (blog), 18 janvier 2021. https://actu.dalloz-etudiant.fr/a-la-une/article/affaire-benalla-preuve-penale-nest-pas-irreguliere-la-preuve-dont-les-conditions-de-recueil/h/5595effa47677125bfd0c2341f9b0076.html.

[107] « Enoncé du moyen (...) 2°/ que c'est en violation de ces mêmes dispositions et sans justifier sa décision que la chambre de l'instruction s'est abstenue de toute prise en compte des circonstances particulières de l'espèce, exposées dans les écritures, liées tant à l'objet et au contexte de l'enregistrement qu'à ses caractéristiques techniques dégagées par expertise au cours de l'enquête, ***dont il résultait que des doutes sérieux existaient quant à l'intervention d'une autorité publique dans sa confection****, ce qui compromettait nécessairement sa régularité ».*

[108] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62533%22]}

[109] Conformément au tableau réalisé en page 30

§1. Décisions de justice liées à de la fraude fiscale étayées par des fuites de données

Les fuites de données, de plusieurs types, ont notamment été utilisées dans le cadre d'investigations menées par des journalistes. À titre d'exemple, les OFFSHORE LEAKS[110] (fuite de donnée par lanceurs d'alerte) ont été utilisées dans de nombreuses enquêtes du journal LE MONDE pour mettre en lumière des réseaux d'évasion et de fraude fiscale à l'international[111]. Également, les YANDEX LEAKS (fuite de données provenant du site BREACH FORUM[112]) ont été exploités et recoupés avec d'autres *leaks* par les journalistes anglais de BELLINGCAT pour exposer les réseaux d'officiers du renseignement militaire russe (GRU) impliqués dans le piratage informatique d'Organisation pour l'interdiction des armes chimiques[113] (OPCW) et l'empoisonnement d'Alexey Navalny[114]. La section ci-après aura pour but d'identifier si de tels éléments ont déjà été utilisés auprès de la justice française par des parties publiques, ainsi que leurs réceptions.

A. L'aide apporté par les OFFSHORE LEAKS en France

1. Une perquisition pour éviter le recel : comment la DNEF a manœuvré pour utiliser les SWISS LEAKS

Dans une affaire de fraude fiscale (Cour de cass, Chambre crim, 6 novembre 2019) résultant des SWISS LEAKS, l'appelant estimait que la saisie par la Direction Nationale des Enquêtes Fiscales (DNEF) de fichiers soustraits à la

---

[110] Nom regroupant l'ensemble des fuites de données reçues par le Consortium international des journalistes d'investigation (ICIJ) : Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers.

[111] LE MONDE. « OFFSHORE LEAKS LEMONDE », s. d. https://www.lemonde.fr/offshore-leaks/.

[112] Burgess, Matt. « Leaked Yandex Code Breaks Open the Creepy Black Box of Online Advertising », aout 2023. https://www.wired.co.uk/article/yandex-leaks-crypta-ads.

[113] Toler, Aric. « Food Delivery Leak Unmasks Russian Security Agents ». BELLINGCAT (blog), 1 avril 2022. https://www.bellingcat.com/news/rest-of-world/2022/04/01/food-delivery-leak-unmasks-russian-security-agents/.

[114] Bellingcat Investigation Team. « Russian Vehicle Registration Leak Reveals Additional GRU Hackers ». BELLINGCAT (blog), 22 octobre 2020. https://www.bellingcat.com/news/uk-and-europe/2020/10/22/russian-vehicle-registration-leak-reveals-additional-gru-hackers/.

banque HSBC Private Bank à Genève par Hervé Falciani s'apparentait à du recel et que l'administration fiscale les avait elle-même confectionnés[115].
Il était ainsi demandé, en vertu d'un procès loyal, la mise à l'écart de ces documents au cours des débats.

La Cour de cassation a affirmé que l'exploitation de fichiers informatiques provenant d'une perquisition, indépendamment de leur origine première, ne s'apparente pas à du recel et ne trouble aucunement le principe de loyauté de la preuve[116].

2. Un emploi qui se normalise avec les PANAMA PAPERS

Au sujet des PANAMA PAPERS, il est possible d'identifier deux décisions de justice rendues par des juridictions pénales (Cour de cass, chambre crim, 21 novembre 2018 & Cour de cass, Chambre crim, 22 mars 2023) dans lesquelles il est possible d'apprendre que le PNF avait débuté certaines de ses enquêtes via ces fuites. Également, il est possible d'observer que les PANAMA PAPERS ont aussi été utilisés auprès de juridictions civiles (Cour de cass, Chambre commerciale, 7 juillet 2020 & Cour d'appel d'Aix-en-Provence, 2 juin 2022) par la DNEF. Le service d'enquête s'est notamment appuyé sur les adresses de domiciliation des sociétés présentes dans les PANAMA PAPERS pour effectuer des recoupements d'information et sanctionner des entreprises.

Ces affaires pénales montrent qu'il est effectivement possible pour des parties publiques de réutiliser dans leurs enquêtes des fuites de données issues de lanceurs d'alerte.

Cependant, la recherche documentaire effectuée sur l'utilisation de fuites de données d'autres catégories, comme celles utilisées par BELLINGCAT, n'ont pas

---

[115] Voir à ce sujet l'arrêt : Cour de cass, Chambre crim, du 6 novembre 2019

[116] « Attendu que sur la validité des éléments de preuve, l'arrêt énonce ***que ne peut s'analyser comme une confection d'éléments de preuve par une autorité publique, le rapprochement et la transcription de données informatiques par l'administration fiscale dans des fiches de synthèse ayant pour seul objet d'en matérialiser le contenu*** *; que les juges retiennent que les allégations de vol ou de recel de données par l'administration fiscale, la police française et les services spéciaux se fondant sur les seules déclarations prêtées à M. S... V... qu'aucun autre élément tant technique que factuel ne vient étayer, ne sauraient suffire à établir que l'administration soit intervenue dans l'élaboration ou l'obtention des éléments de preuve contestés avant que ceux-ci ne soient appréhendés lors de la perquisition puis exploités dans le cadre de l'enquête ; que la cour d'appel en déduit que l'administration fiscale* ***ne saurait se voir reprocher un quelconque manquement au principe de loyauté de la preuv****e, les fichiers HSBC ne revêtant intrinsèquement aucun caractère frauduleux ni illicite les privant de toute valeur probante »*

permis d'identifier une utilisation similaire par des parties publiques dans leurs enquêtes[117].

L'accès à des *leaks* similaires s'avère simple, notamment via le site DDOS SECRET de la cyber militante et journaliste Emma Best dont le credo est consacré à l'archivage et à la diffusion libre de fuites de données d'intérêt public[118]. Plusieurs jeux de données en lien avec des thématiques financières et d'évasion fiscale y sont disponibles[119].

B. Affaires impliquant des données issues d'attaques aux rançongiciels

Suivant la même logique, qu'en est-il pour les *leaks* issues d'attaques aux rançongiciels, qui constituent le centre ce cette réflexion ? Ont-ils déjà été utilisés par des parties publiques dans des enquêtes ? Malheureusement, aucune information en ce sens n'a pu être identifiée. Cependant, il est possible de trouver la trace d'un litige français en faisant mention. L'étude de ce dernier, bien que jugé au civil et opposant deux parties privées, permettra toutefois d'apprécier comment ces données ont été reçues et les objections qu'elles ont pu susciter.

1. DRAHI LEAKS : un premier cas en la matière jugé au civil

Les DRAHI LEAKS, soit l'assemblage des fuites de données prévenantes des rançongiciels HIVE et ROYAL HOUSE analysés par les journalistes du site REFLET (REBUILS.SH), ont été portés en justice en 2022. Sans craindre un effet Streisand[120], la société française de télécommunication a effectivement intenté une action à l'encontre du journal afin de faire supprimer les articles écrits au sujet des DRAHI LEAKS et de les enjoindre à ne plus en publier de nouveaux. L'affaire a été portée auprès de la cour d'appel de Versailles (Cour d'appel de Versailles, 19 janvier 2023, RG 22/06176). Une première pour ces rançongiciels qui se retrouvent au coeur d'un procès, non pas pour leurs attaques en tant que telles, mais pour ce que des tiers en on fait.

---

[117] Sur des décisions de justice au niveau Français et européen grâce au portail E-JUSTICE de l'Union Européenne (https://e-justice.europa.eu/home) et le site PAPPERS (https://justice.pappers.fr/) donnant un accès aux données de la Cour de cassation, du Conseil d'État de la DILA et de certaines Cours d'Appel en France.

[118] Voir notamment la présentations des membres fondateur lors de la conférence DEFCON en 2022 https://www.youtube.com/watch?v=3YtQXTNGJLU

[119] Il est possible d'identifier 6 leaks à ce sujet : DJC Accountants, Kallias and Associates, Odebrecht, Sberbank of Russia, Myanmar Financials, RKPLaw, Sherwood: Cayman National Bank and Trust.

[120] https://fr.wikipedia.org/wiki/Effet_Streisand : « L'effet Streisand désigne un phénomène médiatique involontaire. Il se produit lorsqu'en voulant empêcher la divulgation d'une information que certains aimeraient cacher, le résultat inverse survient, à savoir que le fait caché devient notoire. »

2. Une protection des sources (ouvertes)

Dans son argumentaire, la société éditrice déclare que ces informations, consultables publiquement et issues d'une attaque informatique, ont pu être portés à sa connaissance par une sources « *Elle (REBUILD.SH) entend utiliser "le secret des sources" protégé par l'article 2bis de la loi sur la presse du 29 juillet 1881, pour indiquer que ces données piratées ont pu lui être communiquées par un tiers qui les aura lui-même téléchargées, contestant les avoir elle-même téléchargées ou reproduites dans ses articles* ». Les journalistes n'ignoraient cependant pas leurs origines, il est effectivement bien mentionné dans les articles que HIVE et RANSOM HOUSE en sont les parents. Le contournement de la notion de recel s'avère dès lors plus compliqué.

3. L'accusation de recel d'atteintes à un STAD

L'aspect loyal et licite des documents utilisés dans les articles ainsi que la recherche d'une responsabilité pénale n'était pas au centre du litige. Cependant, il est intéressant de constater que la société ALTICE, dans sa défense, accusait les journalistes de REFLET de recel « *Selon Altice, Rebuild en rédigeant les articles litigieux qui reprennent les données piratées issues d'atteintes au secret des correspondances et qui ont pu augmenter son lectorat, a également commis une infraction à l'article 321-1, alinéa 2 du Code pénal qui incrimine le "recel profit" en bénéficiant de données issues d'une atteinte à un STAD ».* En réponse, la société REBUILD.SH dresse un parallèle intéressant entre « *leaks* » de lanceurs d'alertes communiqués à des journalistes uniquement, et « leaks » de pirates informatiques diffusés sans restriction *« Elle (RUIBUILD.SH) conteste également toute idée de "recel profit", affirmant que c'est l'essence même du journalisme d'investigation qui est ainsi mise en cause et qui s'illustre pourtant dans les articles relatifs aux « panamas papers », « Macronleaks », « wikileaks », « footballleaks » ou « luxleaks » ».*

En tout état de cause, la Cour d'appel a considéré que la défense des journalistes ne permettait pas d'écarter le recel quant à leur utilisation de ces documents[121].

C. Les contre-mesures applicables pour des services d'enquête

Pour l'heure, la jurisprudence au sujet de la réutilisation de fuites de données issues d'attaques aux rançongiciels est très maigre. Un seul cas, jugé au civil et opposant deux entités privées a pu être identifié. Aucune affaire pénale

[121] *"Ce serait en rajouter au texte que d'exiger "un lien direct entre l'introduction dans le STAD et l'acte subséquent de détention, reproduction, transmission, suppression ou modification".*
Les autres moyens soulevés par Rebuild ne permettront pas d'écarter ce recel »

impliquant une partie publique n'a été recensée. Tandis que ces dernières peuvent, selon le CPP et la doctrine en vigueur, inclure dans leurs investigations des éléments déloyaux, l'appréciation par les magistrats de ce type de données s'avère aventureuse. Bien que ces données soient publiques, cela tient notamment à l'absence de cas similaires sur le sujet, de l'aspect clairement délictuel et du moyen d'accès à cette donnée, via TOR et le « *dark net* »[122], qui pâtit d'une image encore très négative dans l'imaginaire populaire[123]. Pour les services d'enquête financière ne souhaitant pas faire un tel pari, des martingales peuvent être envisagées. Ces dernières pourront permettre d'arriver au même résultat sans apparaître comme exposées directement aux pirates informatiques. L'analyse de l'affaire ALTICE VS REBUILD.SH et des enquêtes au sujet des OFFSHORE LEAKS permettront d'apporter des réponses à ce sujet.

1. La reprise d'articles

En se référant aux articles publiés par REFLET (REBUILD.SH), STREET PRESS et BLAST, qui reprennent l'essentiel des informations au sujet des DRAHI LEAKS et qui en publient même des extraits, il n'est pas forcément nécessaire pour un service d'enquête de refaire l'ensemble du travail a partir de la donnée brute, et se risquer à ce que cette donnée soit remise en cause lors des débats. Les articles de presse peuvent être des pièces versées au dossier et soumis aux débats.

À titre d'exemple, dans l'affaire de la DNEF pour laquelle les PANAMA PAPERS avaient été utilisés, et qui avait été portée en cassation (Cour de cass, Chambre commerciale financière et économique, 7 juillet 2020), des articles de presse figurent au dossier « *sur le site https://reporterre.net , il est indiqué que « le préfet M.. O... a rejoint le cabinet de lobbying T... C... Conseil en qualité de Senior Advisor (...) où il pourra utiliser les connaissances acquises au service de l'Etat au profit des grandes entreprises ». (Pièce n° 7 bis) ; (...) Dans un article publié sur le site d'accès public https://www.intelliqenceonline.fr. la société 4 A INTERNATIONAL est présentée comme le « lobbyiste de la défense israélienne en France » (Pièce n° 11)* »

Seul bémol à cette pratique, il faut que les éléments liés à l'enquête aient été médiatisés, ce qui ne concerne pas toutes les affaires.

---

[122] ONION SERVICES, le dark net étant un mot médiatique

[123] Perrat, Jean-François. « Un « Deep / dark web » ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor ». Netcom, no 32-1/2 (16 décembre 2018): 61-86. https://doi.org/10.4000/netcom.3134.

2. Le blanchiment via des droits de communication ou des réquisitions

Autre technique pouvant être mise en oeuvre lorsque que l'on ne souhaite pas reprendre directement les données dérobées et livrées gracieusement pas des cybercriminels : le droit de communication ou la réquisition divinatoire[124]. La consultation des données publiées peut permettre d'identifier des documents matérialisant certaines infractions ou manquements déclaratifs.

Si ces documents proviennent de professionnels assujettis en France ou pouvant être atteints par une réquisition, un droit de communication ou une demande adressée officiellement peut permettre de récupérer ces informations de manière totalement légitime. Ce genre de technique permettant de « blanchir l'information », utilisée notamment par des services de police pour protéger leurs sources humaines[125], permet de faire rejaillir l'information par une voie tout à fait légale, n'appelant aucune objection quand a son origine. La thèse sur le renseignement financier du chercheur Killian Chaudieu décrit parfaitement ce mécanisme : « *Ici, l'analyse du CANAFE[126] permet aux APAL d'obtenir des informations financières spécifiques, auxquelles ils n'ont pas accès sans autorisations judiciaires, pour justement motiver ces demandes et pouvoir ensuite obtenir et utiliser légalement ces informations comme preuves. Cette manière de « blanchir l'information » qui revient à demander et obtenir par voie légale une information dont on a déjà eu accès de manière informelle, est couramment utilisée par les APAL – au Canada comme en Suisse – dans le cadre de leurs enquêtes* »[127].

---

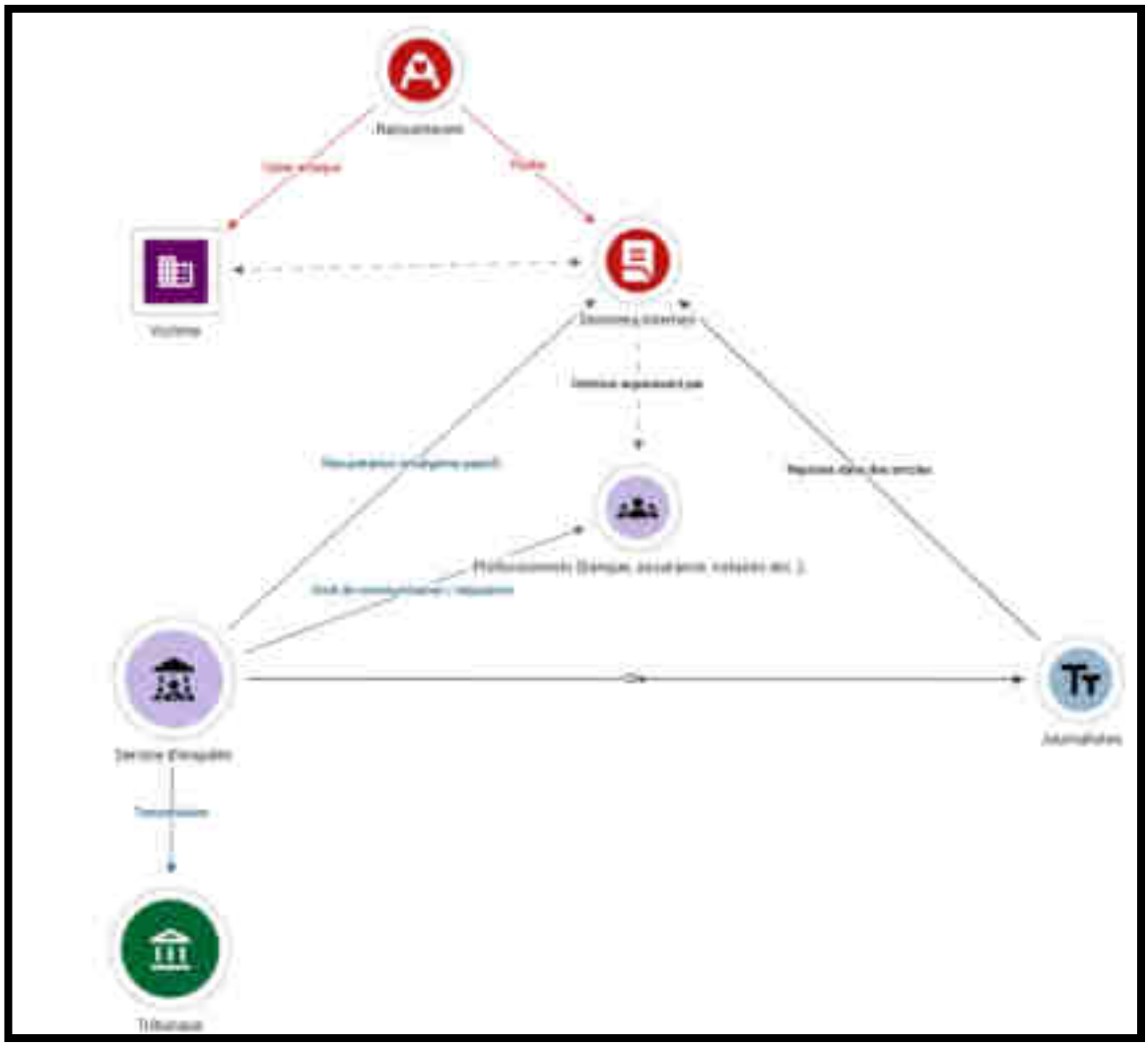
[124] *«Qui relève de la faculté de deviner, qui la manifeste ou en est le produit » selon le CNRTL* https://www.cnrtl.fr/definition/divinatoire

[125] *Franssen, Mathilde, 2020, Quels sont les avantages et limites que présente la méthode particulière de recherche de recours aux indicateurs, utilisée par les enquêteurs, selon la perception de certains acteurs concernés ? Rapport, Université de Liège* https://matheo.uliege.be/bitstream/2268.2/10071/4/Travail%20de%20fin%20d%27%C3%A9tudes%20-%20Franssen%20M.pdf

[126] *Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) est l'unité du renseignement financier et le superviseur en matière de la lutte contre le blanchiment d'argent et le financement des activités terroristes du Canada.*

[127] *Chaudieu Killian, 2022, À quoi sert le renseignement financier ? De la trace financière à la « fabrique de la criminalité » en Suisse et au Canada. Thèse, Université de Lausanne* https://serval.unil.ch/resource/serval:BIB_67A7C3CFC73F.P001/REF.pdf

Le graphique ci après, réalisé à l'occasion de ce mémoire synthétise les actions présentées dans ce chapitre :



(Graphique réalisé par l'auteur de ce mémoire l'aide de l'outil OSINT-TRACKER[128])

Conclusion du chapitre II

En France, le Code de procédure pénale et la jurisprudence permettent aux parties publiques d'user de stratagèmes passifs dans le recueil de la preuve. Souvent qualifiées de « provocation à la preuve », ces actions permettent de verser en procédure des éléments qui auraient été considérés comme déloyaux lors de procédures civiles. Il est possible de citer comme exemple de stratagèmes ayant été validés, l'infiltration de policiers au sein de structures criminelles ou la remise d'enregistrements audio réalisés dans des conditions incertaines par des

[128] https://www.osintracker.com/

tiers. L'incitation demeure le seul rubicond à ne pas franchir. Ainsi, cette possibilité permet donc de récupérer des données librement accessibles, comme celles issues d'attaques aux rançongiciels.

Tandis que des exemples de réutilisation de fuites de données (OFFSHORE LEAKS notamment) par des parties publiques ont pu être identifiés, aucune affaire similaire ne mentionne l'utilisation de données issues d'attaques aux rançongiciels, épineuses tant elles sont liées à des infractions (atteinte aux STAD, extorsion, recel). Pour l'heure, on ne sait donc si l'aspect public de ce type de « *leaks* » pourrait l'emporter sur son origine délictuelle. Toujours est-il qu'en s'écartant d'une simple réutilisation, dans l'idée de ne pas exposer clairement l'origine douteuse de ces données et de se prémunir de toute objection, les services d'enquête financière peuvent blanchir la source de ces informations, par le biais des droits de communication ou des réquisitions par exemple.

Conclusion générale

Dans le cadre d'affaires pénales de nature financières, les données issues d'attaques aux rançongiciels comportent plusieurs avantages. Leurs utilisations par des services d'enquête s'avèrent possibles, mais délicates. Effectivement, le Code de procédure pénale et la jurisprudence en vigueur permettent aux parties publiques de verser en procédure des éléments qui auraient été jugés irrecevables dans des affaires civiles. Recueillies d'initiative ou après avoir sollicité l'accord de la procureure de la République, ces informations collectées via des stratagèmes peuvent jouer un rôle important dans le cadre d'enquêtes complexes. Il n'en demeure pas moins que ces éléments sont souvent critiqués et remis en cause lors des débats contradictoires, notamment pour leur aspect déloyal. Bien que pour l'heure aucune affaire pénale s'appuyant sur des informations issues de cyber attaques aux rançongiciels ne soit connue, il est probable qu'elles subissent les même critiques. Relevant de la catégorie des fuites de données (*leaks*) elles sont cependant à différencier des autres sources de cette grande famille, qu'il a été possible de mieux catégoriser au cours de cette recherche. Bien qu'entièrement publiques ces informations découlent en effet directement d'infractions perpétrées via des rançongiciels et sont diffusées sur ce qui est appelé, a tort, le « *dark-web* ». Hors des tribunaux, plusieurs journalistes ont déjà utilisé ce type de ressources pour mener à bien leurs investigations, notamment dans un cadre financier. Pouvant blanchir l'origine de ces informations et éviter ainsi toute accusation de recel, par le recours au « secret des sources des journalistes», un mécanisme similaire peut être entrepris par un service d'enquête. Ce dispositif peut s'opérer au moyen de droits de communication ou de réquisitions, permettant ainsi l'obtention de certains documents d'intérêts constatés dans la fuite de donnée par une voie plus régulière. Ce constat laisse donc à penser que ces données présentent un intérêt dans le cadre d'enquêtes financières. Les stratagèmes de recueil passif de la preuve permettront leurs utilisation en l'état. Cependant, aux vues des moyens à la disposition des services

d'enquêtes, ces informations pourront être plus aisément employées au travers d'un processus de blanchiment de l'information, à l'image de ce qui se fait traitement des sources humaines dans les enquêtes judiciaires.
Aussi, la recherche aurait gagné à inclure l'avis de professionnels du monde judiciaire, magistrats, officiers de police judiciaire, assistants spécialisés par exemple. Comment sont perçus les stratagèmes par les magistrats ? À quel moment de l'enquête sont-ils utilisés ? L'OSINT est-il considéré comme un renseignement à part entière ? Quelle doctrine d'emploi y est associée ? Les réponses à ces question auraient permis d'être plus exhaustif et précis sur les questions des procédures vis-à-vis des stratagèmes et de la conception de l'OSINT, qui est le champ de recueil des fuites de données par rançongiciels, dans le monde judiciaire.

Pour faire suite à ce mémoire, il serait intéressant de se pencher juridiquement sur l'utilisation, cette fois-ci consciente, de pirates informatiques par des entités privés dans le cadre de procès, via les opérations de type « *Hack-for-hire* ». Les longs et tumultueux litiges entre la Ras Al Khaimah Investment Authority et Farhad Azima, impliquant la société CYBERROOT[129], de même que celui opposant Moukhtar Abliazov et la République du Kazakhstan, portés en France jusqu'au Conseil d'Etat avec l'aide du mystérieux[130] site KAZAWORD, apparaissent à ce sujet comme deux cas intéressants. Plus encore, une étude comparative à mi-chemin entre l'analyse juridique, économique et politique des juridictions permissives, de leurs fonctionnements, ainsi que leurs places dans la stratégie géopolitique globale des États dont elles dépendent, s'avérerait opportune. Plusieurs juridictions de ce type, ne stipulant aucune ligne directrice quant à l'admissibilité de la preuve, semblent ainsi savamment choisies lors de l'élaboration des clauses attributives de compétence pour faciliter tout type d'apport de la preuve, dont le piratage, en cas de discorde. Sur ce point, l'analyse du fonctionnent de la Commission Chinoise d'Arbitrage de l'Economie et du Commerce International (CIETAC) et l'approfondissement de l'article « *Hacking the system: admissibility of evidence from cyberattacks in arbitration* » publié en juillet 2023 dans la revue Arbitration Review of the Americas, semble une bonne base de départ[131].

---

[129] *A ce sujet voir notamment l'article de David D. Kirkpatrick publié le 1 juin 2023 dans The New-Yorker intitulé « A Confession Exposes India's Secret Hacking Industry ». Disponible ici : https://www.newyorker.com/news/annals-of-crime/a-confession-exposes-indias-secret-hacking-industry*

[130] *Vasset et Gastineau op.cit p26*

[131] *Article disponible à l'adresse suivante : https://globalarbitrationreview.com/review/the-arbitration-review-of-the-americas/2024/article/hacking-the-system-admissibility-of-evidence-cyberattacks-in-arbitration*

En courbant le regard et en croisant les thématiques, cette recherche permet donc l'identification d'un moyen permettant à des enquêteurs d'accéder à des données difficilement accessibles par d'autres méthodes, tout en consolidant l'apport de l'OSINT dans le cadre d'enquêtes financières et en précisant la notion de « fuite de donnée ».

Avec du recul, cette étude est aussi celle d'un engrenage dans lequel des criminels concourent à la sanction d'autres criminels, sans le savoir et en facilitant le travail des enquêteurs. La « téléperquisition » ayant déjà été réalisée, d'une certaine manière, par les cyber pirates de façon autonome.

Bien que protégés par des lois avantageuses dans des ETNC paradisiaques et exploitant à leurs fins l'absence d'homogénéité sur la lutte contre l'évasion fiscale, les sociétés fiduciaires et cabinets de conseils spécialisés dans l'aide à l'évasion fiscale peuvent quand même révéler leurs secrets, pour le plus grand intérêt des journalistes et des enquêteurs.

Bibliographie

- « 2021 Trends Show Increased Globalized Threat of Ransomware ». Cybersecurity and Infrastructure Security Agency (CISA), février 202apr. J.-C. https://www.cisa.gov/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf.

- Abrams, Lawrence. « Computer hardware giant GIGABYTE hit by RansomEXX ransomware ». Bleeping Computer (blog), s. d. https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/.

- Addesa-Pelliser, Elena. « Le Gafi, l'investigation financière criminelle (IFC) et l'analyse financière criminelle (AFC) : un changement paradigmatique à l'oeuvre. » Université de Strasbourg, 2019. https://theses.hal.science/tel-03525636/document.

- Agence nationale de la sécurité des systèmes d'information. « Attaques par rançongiciels, tous concernés. », 4 septembre 2020. https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes.

- Audibert, Matthieu. « La pénétration du droit pénal dans l'espace privé. La captation de données informatiques », Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 91-103.

- « Along the sanctioned persons :KERIMOV Suleyman Abusaidovich », s. d. https://sanctions.nazk.gov.ua/en/sanction-person/741/.

- ALPHV RANSOMWARE, janvier 2023. www.vqifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd.onion.

- Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire », INTR1802937A § (2018). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036887904.

- Bellingcat Investigation Team. « Russian Vehicle Registration Leak Reveals Additional GRU Hackers ». BELLINGCAT (blog), 22 octobre 2020. https://www.bellingcat.com/news/uk-and-europe/2020/10/22/russian-vehicle-registration-leak-reveals-additional-gru-hackers/.

- Beroule, Marie. « La loyauté de la preuve pénale ». Mémoire de recherche, AIX-MARSEILLE UNIVERSITE FACULTE DE DROIT ET DE SCIENCE POLITIQUE, 2022. https://dumas.ccsd.cnrs.fr/dumas-03541064/document.

- Bertran, Marie-Gabrielle. « Illustration des apports et limites de l'usage des sources ouvertes à travers le cas de la Russie ». Hérodote 186, no 3 (2022): 85-99.

- Bogdan, Bodnar. « Les avocats de plus en plus ciblés par les hackers, alerte l'ANSSI ». Numérama (blog), 27 juin 2023. https://www.numerama.com/cyberguerre/1428430-les-avocats-de-plus-en-plus-cibles-par-les-hackers-alerte-lanssi.html.

- Burgess, Matt. « Leaked Yandex Code Breaks Open the Creepy Black Box of Online Advertising », aout 2023. https://www.wired.co.uk/article/yandex-leaks-crypta-ads.

- Cambridge Dictionary. « Leak defintion », s. d. https://dictionary.cambridge.org/fr/dictionnaire/anglais-francais/leak.

- Chaudieu Killian, 2022, À quoi sert le renseignement financier ? De la trace financière à la « fabrique de la criminalité » en Suisse et au Canada. Thèse, Université de Lausanne https://serval.unil.ch/resource/serval:BIB_67A7C3CFC73F.P001/REF.pdf

- CNRTL. « Définition du mot "fuite" ». Centre national de ressources textuelles et lexicales (blog), https://www.cnrtl.fr/definition/fuite.

- Code de procédure pénale, Articles 56 (2004). https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006151876/.

- Commission d'accès aux documents administratifs. « Les secrets protégés par la loi », s. d. https://www.cada.fr/particulier/les-secrets-proteges-par-la-loi.

- Conclusions du Conseil relatives à la liste révisée de l'UE des pays et territoires non coopératifs à des fins fiscales (2023). https://data.consilium.europa.eu/doc/document/ST-6375-2023-INIT/fr/pdf.

- Conseil de l'Europe. Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales telle qu'amendée par les Protocoles n° 11 et n° 14 (1950).

- Conseil de l'Union européenne. « Chronologie - liste de l'UE des pays et territoires non coopératifs », 17 octobre 2023. https://www.consilium.europa.eu/fr/policies/eu-list-of-non-cooperative-jurisdictions/timeline-eu-list-of-non-cooperative-jurisdictions/.

- Consortium international des journalistes d'investigation. « OffshoreLeaks », s. d. https://offshoreleaks.icij.org/pages/database.

- Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime du 9 novembre 1990 (1990). https://rm.coe.int/168007bd2f.

- Council of the European Union. COUNCIL IMPLEMENTING REGULATION implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, 7125/22 § (2022). https://data.consilium.europa.eu/doc/document/ST-7125-2022-INIT/en/pdf.

- Cour européenne des droits de l'Homme. Arret du 27 mars 1996 AFFAIRE GOODWIN c. ROYAUME-UNI (1996). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62533%22]}.

- ———. ARRÊT du 28 juin 2012 AFFAIRE RESSIOT ET AUTRES c. FRANCE (s. d.). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-111670%22]}.

- Cox, Joseph. « Pro-Russia Conti Ransomware Gang Targeted, Internal Chats Leaked ». VICE MAGAZINE, 28 février 2022. https://www.vice.com/en/article/z3ng84/pro-russia-conti-ransomware-messages-leaked.

- « CYBER THREAT OVERVIEW 2022 ». Rapport annuel. Paris: Agence nationale de la sécurité des systèmes d'information, janvier 2023. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf.

- Cybersecurity and Infrastructure Security Agency. « #StopRansomware Guide », s. d. https://www.cisa.gov/stopransomware/ransomware-guide.

- « Definitive guide to ransomware 2023 ». IBM SECURITY, mai 2023. https://www.ibm.com/downloads/cas/OW1D41LK.

- Department of Justice. « Rewards for Justice Up to $10 million », s. d. https://rewardsforjustice.net/rewards/conti/.

- Direction de l'information légale et administrative (Première ministre). « Ransomware ou rançongiciel ». service-public.fr (blog), 15 mars 2022. https://www.service-public.fr/particuliers/vosdroits/F34129.

- Dreyer, Emmanuel. « Chapitre 1. Le recel du produit des atteintes aux biens », , Droit pénal spécial. sous la direction de Dreyer Emmanuel. Ellipses, 2016, pp. 565-580. https://www.cairn.info/droit-penal-special--9782340014015-page-565.htm

- « ÉTAT DE LA MENACE RANÇONGICIEL À L'ENCONTRE DES ENTREPRISES ET DES INSTITUTIONS ». Agence nationale de la sécurité des systèmes d'information, 1 septembre 2021.

- « European Companies Search Engine : NorthData », s. d. https://www.northdata.com/?id=6132755186.

- EUROPOL. « Cybercriminals stung as HIVE infrastructure shut down », 26 janvier 2023. https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.

- @FalconFeedsio. Twitter (blog), 28 octobre 2022. https://twitter.com/FalconFeedsio/status/1585868867817312256.

- FBI Press room. « FBI Leads Action Against "CryptoLocker" Ransomware », juin 2014. https://ucr.fbi.gov/washingtondc/news-and-outreach/press-room/this-month/this-month-at-the-wfo-june-2014.pdf F.

- FINAPORT. « OUR MISSION », 1 octobre 2023. https://data.consilium.europa.eu/doc/document/ST-6375-2023-INIT/fr/pdf.

- Franssen, Mathilde, 2020, Quels sont les avantages et limites que présente la méthode particulière de recherche de recours aux indicateurs, utilisée par les enquêteurs, selon la perception de certains acteurs concernés ? Rapport, Université de Liège https://matheo.uliege.be/bitstream/2268.2/10071/4/Travail%20de%20fin%20d%27%C3%A9tudes%20-%20Franssen%20M.pdf

- Freeman, Lindsay. « Hacked and Leaked: Legal Issues Arising From the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases ». UCLA Journal of International Law and Foreign Affairs, Human Rights Center, UC Berkeley School of Law, 25, no 2 (2021): 45-91. https://escholarship.org/content/qt5b87861x/qt5b87861x_noSplash_48c123785a2ad83b4be92dd72497af91.pdf.

- GAFI. « Operational Issues - Financial Investigations Guidance », juin 2022. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf.

- « GAFI/FATAF:Operational Issues - Financial Investigations Guidance », juin 2012. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf.

- Glace, Demetria. Leaked recipes: the cookbook. JBE <3 food. Paris: JBE books, 2020.

- Glover, Claudia. « FBI joins investigation into Continental ransomware attack ». TECHMONITOR.AI (blog), 23 novembre 2022. https://techmonitor.ai/technology/cybersecurity/continental-cyberattack-ransomware-lockbit-fbi.

- Guéniat, Marc, et Antoine Harari. « Le réseau suisse du prince des oligarques ». LE TEMPS (blog), 17 septembre 2022. https://www.letemps.ch/suisse/reseau-suisse-prince-oligarques.

- Guiton, Amaelle. « Rançongiciels: un chantage qui chiffre sérieusement ». Libération, 22 novembre 2022. https://www.liberation.fr/societe/rancongiciels-un-chantage-qui-commence-a-serieusement-chiffrer-20221123_CABNEQARZBH5JLNASFGVESFFNI/.

- Hervieu, Merryl. « Policier infiltré : tant qu'il n'est pas pousse au crime, le stratagème n'attente pas à la loyauté de la preuve ». DALLOZ (blog), 20 janvier 2020. https://actu.dalloz-etudiant.fr/a-la-une/article/policier-infiltre-tant-quil-nest-pas-pousse-au-crime-le-strategeme-nattente-pas-a-la/h/16019c32d59c4e5bed99f609ca39d4c2.html.

- Hope, Alicia. « United States Nuclear Missile Contractor Hit by Maze Ransomware Attack ». CPO magazine (blog), s. d. 11 juin 2020.

- IEEE Computer Society, International Association for Cryptologic Research, et Institute of Electrical and Electronics Engineers, éd. Cryptovirology : Extortion-Based Security Threats and Countermeasures. Los Alamitos, Calif.: IEEE Computer Society Press, 1996. https://www.ieee-security.org/TC/SP2020/tot-papers/young-1996.pdf.

- INTEL 417. « Conti vs. Monti: A Reinvention or Just a Simple Rebranding? », 7 septembre 2022. https://intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding.

- INTEL 417. « LockBit 3.0 Builder Code Leak Points to Another Disgruntled Criminal Employee », 12 octobre 2022. https://intel471.com/blog/lockbit-3-0-builder-code-leak-points-to-another-disgruntled-criminal-employee.

- Lavric, Sabrina. « Affaire Benalla. Preuve pénale : n'est pas irrégulière la preuve dont les conditions de recueil sont restées incertaines ». DALLOZ (blog), 18 janvier 2021. https://actu.dalloz-etudiant.fr/a-la-une/article/affaire-benalla-preuve-penale-nest-pas-irreguliere-la-preuve-dont-les-conditions-de-recueil/h/5595effa47677125bfd0c2341f9b0076.html.

- LE MONDE. « OFFSHORE LEAKS LEMONDE », s. d. https://www.lemonde.fr/offshore-leaks/.

- Les Echos. « Ukraine : Bercy organise la traque des biens des oligarques russes », 1 mars 2022. https://www.lesechos.fr/economie-france/budget-fiscalite/ukraine-bercy-organise-la-traque-des-biens-des-oligarques-russes-1390542.

- LOI n° 2010-1 du 4 janvier 2010 (2010). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000021601325/.

- LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, IOMD2223411L § (2023). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768.

- Lua, Eng Keong, Jon Crowcroft, Marcelo Pias, Sharma Ravi, et Lim Steven. « A Survey and Comparison of Peer-to-Peer Overlay Network Schemes ». IEEE COMMUNICATIONS SURVEY AND TUTORIAL, 31 mars 2004. https://snap.stanford.edu/class/cs224w-readings/lua04p2p.pdf.

- Microsoft Threat Intelligence. TWITTER (blog), janvier 2023. https://twitter.com/MsftSecIntel/status/1620474448494075909?lang=fr.

- Murphy Kelly, Samantha. « The bizarre story of the inventor of ransomware ». CNN Business, 16 mai 2021. https://edition.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html.

- NAEL, Olivier. « La "télé" perquisition - OCLCTIC ». s. d. https://clusif.fr/wp-content/uploads/2015/09/clusif-forensics-2010-teleperquisition-oclctic.pdf.

- Orange Cyberdéfense. « Beating ransomware A comprehensive guide to tackling the cyber extortion threat », 2021. https://www.orange-business.com/sites/default/files/beating-ransomware-solutions-guide.pdf.

- Paganini, Pierluigi. « BlackCat Ransomware gang stole secret military data from an industrial explosives manufacturer ». Security Affairs (blog), 27 janvier 2023. https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html.

- Page, Carly, et Zack Whittaker. « Hackers publish sensitive employee data stolen during CommScope ransomware attack ». TechCrunch (blog), 17 avril 2023. https://techcrunch.com/2023/04/17/hackers-publish-sensitive-employee-data-stolen-during-commscope-ransomware-attack/.

- Parlement Européen. DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, Pub. L. No. 12 aout 2013, L 218/8 (s. d.). https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32013L0040&from=SL.

- Perrat, Jean-François. « Un « Deep / dark web » ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor ». Netcom, no 32-1/2 (16 décembre 2018): 61-86. https://doi.org/10.4000/netcom.3134.

- Prodaft. « Conti Ransomware Group In-Depth Analysis ». Cyber. Suisse: PRODAFT, s. d. https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf.

- Queirós, Óscar. « Armando Pereira e Vaz Antunes presos em casa sem pagar caução ». Jornal de Notícias (blog), 24 juillet 2023. https://www.jn.pt/7993107800/armando-pereira-e-vaz-antunes-presos-em-casa-sem-pagar-caucao/.

- RansomChaT. « **********149576 », s. d. https://ransomch.at/lockbit3.0-**********149576.

- Rellé, Aaron. « Le droit de la preuve en matière pénale ». VILLAGE DE LA JUSTICE (blog), 17 mai 2023. https://www.village-justice.com/articles/droit-preuve-matiere-penale,45864.html.

- Renucci, Jean-François. « Droits de l'homme », Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2014, pp. 843-847. https://doi.org/10.3917/rsc.1404.0843.

- Ruche, Sébastien. « Des hackers russes dévoilent par mégarde les données de plusieurs oligarques ». LE TEMPS (blog), 21 avril 2022. https://www.letemps.ch/economie/finance/hackers-russes-devoilent-megarde-donnees-plusieurs-oligarques.

- « Sanctions List Search », s. d. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=24325.

- Sérgio Azenha, António, et Tânia Laranjo. « Milionário da Altice ganha 32 milhões de euros em esquema suspeito ». Correio da Manhã (blog), 24 juillet 2023. https://www.cmjornal.pt/portugal/detalhe/milionario-da-altice-ganha-32-milhoes-de-euros-em-esquema-suspeito.

- Somé-Blad, 2lodie. « Du leak en tant qu'archive, ou comment le leak est devenu une archive ». Université de Lyon, 2017. https://www.enssib.fr/bibliotheque-numerique/documents/67750-leak-en-tant-qu-archive-ou-comment-le-leak-est-devenu-une-archive-du.pdf.

- Suc, Matthieu. Renault, nid d'espions. Poche 205. Paris: Harper Collins, 2020.

- Também, Leia. « Altice aceitou proposta de Vaz Antunes após recusar uma mais alta ». Jornal de Negócios (blog), s. d. https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/venda-de-data-centers-pode-render-700-milhoes-a-altice.

- « The Anatomy of Targeted Ransomware Attacks ». Danish Centre for Cybersecurity, 16 novembre 2020. https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/cfcs-the-anatomy-of-targeted-ransomware-attacks.pdf.

- Threat & Detection Research Team. « État des lieux de la menace Ransomware au second semestre 2022 ». SEKOIA.IO, 31 janvier 2023. https://blog.sekoia.io/fr/etat-des-lieux-de-la-menace-ransomware-au-second-semestre-2022-par-sekoia-io/.

- Toler, Aric. « Food Delivery Leak Unmasks Russian Security Agents ». BELLINGCAT (blog), 1 avril 2022. https://www.bellingcat.com/news/rest-of-world/2022/04/01/food-delivery-leak-unmasks-russian-security-agents/.

- « TOR METRICS USERS », 22 novembre 2023. https://metrics.torproject.org/userstats-relay-country.html?start=2022-01-01&end=2022-12-31&country=all&events=off.

- TOR PROJECT. « Historique », s. d. https://www.torproject.org/fr/about/history/.

- Touret, Franck. « Corrigé Droit civil ENM 2017 : La loyauté de la preuve dans le procès civil », 2017. https://www.prepa-isp.fr/wp-content/uploads/2018/09/ENM-Annales-Civil-2017.pdf.

- United States of America VS PARK JIN HYOK, also known as (« aka »), « Jin Hyok Park, » aka « Pak Jin Hek, » No. M18- 1479 (s. d.).

- Vasset, Philippe, et Pierre Gastineau. Armes de déstabilisation massive. Paris: Fayard, 2017.

- Wagner Ramsdell, Kellyn A, et Kristin E. Esbeck. « EVOLUTION OF RANSOMWARE ». The MITRE Corporation, juillet 2021.

- Yenouskas, Joseph F, et Levi W Swank. « Emerging Legal Issues in Data Breach Class Actions ». The Business Lawyer 73, no 2 (2018). https://www.americanbar.org/groups/business_law/resources/business-law-today/2018-july/emerging-legal-issues-in-data-breach-class-actions/.

- ZDNET. « Un constructeur aéronautique paralysé par un ransomware », 13 juin 2019. https://www.zdnet.fr/actualites/un-constructeur-aeronautique-paralyse-par-un-ransomware-39885909.htm.

Table des matières

Résumé

Objet de cette recherche, les fuites de données issues d'attaques aux rançongiciels à double extorsion ont significativement augmenté au cours de ces cinq dernières années. Ce phénomène récent amène à considérer l'utilisation d'un nouveau type de sources dans le cadre d'investigations financières de nature pénale. La mise en ligne de ces données par les cyber rançonneurs se distingue en effet des moyens conventionnels dont dispose un service d'enquête. Dans le cadre d'affaires portés en justice, l'origine délictuelle de ces informations provenant d'attaques informatiques, n'est pas à éluder. Cette recherche tente donc de répondre, à travers une analyse documentaire du code de procédure pénale, de la jurisprudence, de la doctrine et des articles de presse, à trois grandes interrogations : Est-il possible pour un service d'enquête d'utiliser ces informations ? Si oui, de quel manière ? et, existe t-il des exemples à ce sujet ?

Ainsi, il possible d'affirmer que la collecte et l'utilisation de ces informations réponds au principe de recueil passif de la preuve, par le biais de ce que la jurisprudence qualifie de « stratagème ». Bien qu'aucun cas d'utilisation par des parties publiques lors d'affaires pénales n'ait été identifié, plusieurs journalistes ont utilisé ce type d'informations dans leurs investigations. L'étude d'un jugement rendu par une juridiction civile (Cour d'appel de Versailles, 14ème Chambre, 19 janvier 2023) s'appuyant sur une de ces investigations journalistique a permis de dresser un parallèle avec les moyens dont disposent les services d'enquête pour utiliser des informations non conventionnelles.

Plus encore, cette étude se penche sur un objet encore assez peu exploité dans le cadre de recherches universitaires juridique : l'utilisation des fuites de données comme outils d'aide à l'enquête. A ce sujet, ce mémoire de recherche propose pour la première fois une classification des différentes familles de fuites de données en quatre grandes catégories.

MOTS CLES : Fuite de donné, leaks, ransomware, rançongiciels, investigation, investigation financière, piratage informatique, droit pénal des affaires, réseau tor, OSINT .

CONTACT : mathieu.han-leveau@etu.unistra.fr

Summary

The subject of this research, data leaks from double extortion ransomware attacks, have increased significantly over the last five years. This recent trend leads us to examine the use of a new type of source in criminal financial investigations. The fact that ransomware operators put this data online differs from the conventional tools available to an investigation department. In legal cases, the criminal origin of this information, resulting from cyber-attacks, cannot be avoided. Through a documentary analysis of the French Code of Criminal Procedure, legal precedent, and press articles, this research attempts to answer three major questions: Is it possible for an investigation department to use this information? If so, in what way? And are there any examples?

Thus, it can be assumed that the collection and use of such information complies with the principle of passive gathering of evidence, through what legal precedents classify as "stratagem". Although no public cases of the use of such information in criminal cases have been identified, several journalists have used this type of information in their investigations. The study of a judgment handed down by a civil court (Versailles Court of Appeal, 14th Chamber, January 19, 2023) based on one of these journalistic investigations provided an opportunity to establish a parallel with the resources available to investigative services in using non-traditional information.

Furthermore, this study examines a subject that is still relatively unexplored in legal academic research: the use of leaked data as an investigative tool. In this domain, this research paper presents, for the first time, a categorization of the different families of leaked data into four major categories.

KEYWORDS Data leak, leaks, ransomware, investigation, financial investigation, hacking, criminal business law, tor network, hack and leaks operations, OSINT.

CONTACT : mathieu.han-leveau@etu.unistra.fr