Criminologie, Forensique et Sécurité

www.revue-cfs.net | ISSN : 2813-6098

Organe officiel de l'association internationale des criminologues de langue française (AICLF)

Article régulier

Criminologie, Forensique et Sécurité

2024 | 2 (1) : 4624

https://doi.org/ 10.26034/la.cfs.2024.4624

Le chiffrement des téléphones: implications pour les enquêtes policières et la confidentialité

Mélanie Théorêt[1],David Décary-Hétu[1] et Cloé Gobeil[1]

[1] École de criminologie, Université de Montréal

Contact : melanie.theoret@umontreal.ca

Résumé

Cet article explore les implications de l'utilisation des "dark phones" et de l'écoute électronique dans le contexte des enquêtes policières. Il met en lumière les défis que pose le chiffrement des communications pour la surveillance légale et les efforts d'application de la loi. L'article commence par décrire comment les forces de l'ordre adaptent leurs méthodes pour répondre à l'évolution des technologies de communication sécurisées, utilisées tant par des citoyens respectueux de la loi que par des criminels pour dissimuler leurs activités. Le texte discute ensuite de diverses affaires judiciaires et opérations policières, notamment les cas de Phantom Secure et Encrochat, illustrant les stratégies utilisées pour contourner les mesures de chiffrement et accéder aux communications des suspects. Ces études de cas démontrent la complexité et les implications légales de l'accès aux données chiffrées, soulignant la tension entre la protection de la vie privée et les besoins de la sécurité nationale. Finalement, l'article examine les implications légales et les débats politiques autour de l'accessibilité des communications chiffrées pour les forces de l'ordre, mettant en évidence la nécessité d'un équilibre entre droits individuels et impératifs de sécurité publique. .

Mots clés

Téléphone mobile, téléphone crypté, téléphone fantôme, surveillance, preuves, décisions judiciaires, nouvelles technologies, application de la loi, confidentialité, sécurité des communications, chiffrement

Phone encryption: implications for police investigations and privacy

Abstract

This paper explores the implications of using "dark phones" and electronic eavesdropping in the context of police investigations. It highlights the challenges posed by encryption of communications for legal surveillance and law enforcement efforts. The analysis begins by describing how law enforcement adapt their methods to respond to the evolution of secure communication technologies, used by both law-abiding citizens and criminals to conceal their activities. The paper then discusses various court cases and police operations, including the cases of Phantom Secure and Encrochat, illustrating the strategies used to circumvent encryption measures and access suspects' communications. These case studies demonstrate the complexity and legal implications of accessing encrypted data, highlighting the tension between privacy protection and national security needs. Finally, the paper examines the legal implications and political debates surrounding the accessibility of encrypted communications for law enforcement, emphasizing the need for a balance between individual rights and public security imperatives.

Keywords

Mobile phone, encrypted phone, ghost phone, surveillance, evidence, legal decisions, new technologies, law enforcement, privacy, communication security, encryption

Citation : Théorêt, M., Décary-Hétu, D. (2024) Le chiffrement des téléphones: implications pour les enquêtes policières et la confidentialité. *Criminologie, Forensique et Sécurité*, 2 (1) : 4624.

L'écoute électronique dans le contexte policier

L'écoute électronique est un outil rarement utilisé par les forces policières en Occident, notamment en raison des enjeux liés à la vie privée, ainsi qu'aux coûts financiers et humains qu'elle engendre (Diffie et Landau, 2010). Elle permet cependant aux forces policières d'obtenir des informations essentielles et joue un rôle important dans les enquêtes, notamment dans celles liées au trafic de drogue (Boustead, 2020; Finklea, 2016). En effet, l'écoute électronique produit une preuve difficilement réfutable, qui a un impact important sur la collecte de renseignements criminels, et les délibérations des jurys. Les forces policières possèdent aujourd'hui la capacité de faire de l'écoute électronique sur les lignes téléphoniques terrestres et cellulaires, mais également sur les messages textes et les connexions internet (Christie, 2019). Les forces policières peuvent donc surveiller les communications de suspects sur plusieurs médiums à la fois.

Le développement des capacités d'écoute des forces policières a amené les délinquants à considérer diverses options pour communiquer de manière anonyme, et confidentielle. Certaines applications commerciales de messagerie comme le BlackBerry Messenger et WhatsApp ont ainsi été adoptées afin de rendre l'écoute électronique plus difficile (Cents et Le-Khac, 2020). Ces applications offrent en effet le chiffrement des communications d'utilisateur à utilisateur, ce qui empêche la lecture des messages échangés alors qu'ils transitent par l'internet ou les réseaux cellulaires. Comme les forces policières mettent en place leur système d'écoute sur ces réseaux, le chiffrement des communications d'utilisateur à utilisateur rend caduque les capacités de surveillance (Finklea, 2016). Ce dernier n'est cependant pas une panacée. Tel que démontré dans l'enquête sur le meurtre de Salvatore Montagna (Touzin et al., 2015), les forces policières ont en effet été en mesure d'obtenir l'assistance des propriétaires d'applications commerciales de messagerie pour surveiller leurs utilisateurs à leur insu.

Les dark phones

Devant les limites des télécommunications traditionnelles, et des applications commerciales de messageries, les délinquants se sont tournés vers des fournisseurs de service à la légalité grise pour continuer de communiquer entre eux. Ces fournisseurs offrent un type d'appareil que nous nommerons "dark phones" dans un secteur d'activité qui est en forte croissance depuis les dernières années (Pisaric, 2021a). Selon un sondage mondial sur ce type de produits, le Canada se place en quatrième position, derrière le Royaume-Uni, l'Allemagne et les États-Unis parmi les pays produisant le plus de dark phones (Schneier, Seidel et Vijayakumar, 2016). Les dark phones protègent avant tout de l'écoute électronique (Weinstein, 2015) en communiquant à l'aide de clés de chiffrement uniquement sauvegardées sur les appareils, et non sur les serveurs des fournisseurs de service. Sans ces dernières, toutes les communications sont indéchiffrables. Les dark phones protègent également contre la découverte de preuves en cas de saisie des téléphones. Leur contenu est chiffré en tout temps, ainsi que facilement et rapidement effaçable avec un accès physique au téléphone, ou à distance. Ainsi, même si une organisation policière avait l'autorisation d'un tribunal pour faire de l'écoute électronique sur un dark phone, elle n'aurait dans la plupart des cas pas les capacités techniques pour déchiffrer les communications surveillées. Plusieurs fournisseurs se sont succédé au cours des 10 dernières années, et nous présentons ci-dessous les principaux.

Les dark phones de la compagnie Ennetcom (2013-2016) étaient des appareils BlackBerry modifiés pour n'envoyer et recevoir des messages qu'avec d'autres appareils du même réseau (Pisaric, 2021a). Ces derniers n'avaient pas de microphone et ne pouvaient pas prendre de photos (Regnery, 2020). Afin de pouvoir échanger des messages, les utilisateurs recevaient d'Ennetcom des adresses courriel anonymes par lesquelles les utilisateurs pouvaient communiquer (Pisaric, 2021a). Bien que le chiffrement offert par Ennetcom était de grande qualité, il n'offrait en réalité aucune sécurité, car les clés de chiffrement et les messages étaient conservés sur les serveurs de la compagnie (Cox, 2017). Ennetcom avait par ailleurs la capacité d'effacer à distance tout le contenu des dark phones sur son réseau, et ses administrateurs pouvaient contrôler à distance presque toutes les fonctions des dark phones (Pisaric, 2021a).

Similairement à Ennetcom, Phantom Secure (2008-2018) vendait des téléphones BlackBerry modifiés qui n'avaient plus de microphone, de GPS, d'appareil photo et d'accès à l'internet (Pisaric, 2021a). La compagnie utilisait des logiciels et algorithmes de chiffrement à code source ouvert de dernière génération. Les messages des utilisateurs étaient échangés à travers des serveurs basés à Hong Kong et au Panama, et passaient à travers plusieurs réseaux de relais pour protéger l'anonymat des utilisateurs (Pisaric, 2021a). Afin de s'abonner aux services de Phantom Secure, les clients n'avaient pas besoin de fournir leur nom réel ou toute autre information qui pourrait les identifier, et ils communiquaient ensemble avec des noms d'emprunt en se créant un compte de messagerie anonyme (Pisaric, 2021a).

Les téléphones cryptés d'Encrochat (2016-2020), une compagnie européenne, n'étaient pas connectés à des cartes SIM associées à un compte client pour garantir l'anonymat des utilisateurs (Zagaris et Plachta, 2020). Par défaut, les dark phones s'allumaient avec un système d'exploitation Android standard. Une manipulation permettait cependant de redémarrer le téléphone dans un système d'exploitation chiffré, Encrochat OS. Ce système d'exploitation était camouflé afin de ne pas être détectable lors d'analyses forensiques (Eurojust, 2020; Zagaris et Plachta, 2020). La plupart des téléphones d'Encrochat n'utilisaient pas de caméra, de microphone, de GPS et de prise USB (Eurojust, 2020; Murray, 2021b; Zagaris et Plachta, 2020). Les dark phones ne permettaient donc que l'envoi et la réception de messages textes et d'images, pas d'appels vocaux (Pisaric, 2021a). Ces derniers faisaient transiter tous leurs messages à travers les serveurs de l'entreprise (Regnery, 2020), et ceux-ci étaient effacés automatiquement sur le téléphone du destinataire après lecture. Le service à la clientèle de la compagnie offrait en cas d'urgence de supprimer tout le contenu associé à un utilisateur. En cas de saisie, l'utilisateur pouvait effacer le contenu de son téléphone en entrant un NIP prédéterminé (Eurojust, 2020).

Sky Global (2008-2021) a été fondé en 2008 et a opéré depuis le Canada et les États-Unis (Pisaric, 2021a). Les dark phones de la compagnie fonctionnaient en installant un logiciel de chiffrement qui était caché sur un appareil iPhone, Google Pixel, BlackBerry ou Nokia. Ce logiciel acheminait les messages chiffrés vers des relais basés en France et au Canada, permettant ainsi d'anonymiser la source et la destination des messages (Pisaric, 2021a). Comme pour les autres compagnies, l'appareil photo, le microphone et le GPS étaient désactivés (Pisaric, 2021a). L'application Sky ECC était

stockée sur les téléphones et sécurisée pour la protéger contre les potentiels logiciels malveillants (Pisaric, 2021a). Les messages chiffrés étaient supprimés après 48h quand ils étaient envoyés à un destinataire non joignable et l'entrée d'un mot de passe de secours permettait de supprimer immédiatement tout le contenu de l'appareil (Pisaric, 2021a).

Anom (2021) est apparu en 2021 comme une alternative intéressante aux compagnies qui avaient été visées par des opérations policières dans les dernières années (Pisaric, 2021a). La particularité d'Anom était par contre qu'il s'agissait d'une compagnie créée dans le cadre d'une enquête par des agents de police de l'Australie, des États-Unis et d'Europol afin de surveiller les messages chiffrés échangés par des délinquants (Pisaric, 2021a). Les dark phones contenaient une seule application fonctionnelle de messagerie déguisée en calculatrice qui fonctionnait sur les systèmes d'exploitation Android et qui se mettait en fonction après l'entrée d'un code (Pisaric, 2021a). Les utilisateurs pouvaient, comme pour un téléphone cellulaire régulier, faire des appels vocaux et échanger des textos, des photos, des vidéos et des fichiers, mais de manière sécurisée et anonyme (Pisaric, 2021a).

Les dark phones ont donc été commercialisés comme des appareils ayant des fonctionnalités entièrement sécurisées à l'épreuve de la surveillance et qui assurent une confidentialité complète à leurs utilisateurs (Eurojust, 2020; O'Rourke, 2020; Pisaric, 2021a). Il existe différentes entreprises qui offrent des dark phones dans le monde et bien que leurs fonctionnalités puissent varier, leur objectif principal est le même, soit d'assurer un anonymat et une confidentialité complets à leurs utilisateurs. Les publicités pour ces appareils promeuvent l'effacement instantané de tous les contacts, messages et données, sans mémoire de secours (O'Rourke, 2020; Zagaris et Plachta, 2020). Cela va donc au-delà des promesses des applications de messagerie commerciales comme WhatsApp et Telegram qui chiffrent les communications, mais qui en conservent toutes les traces (Boustead, 2020; Graham, 2016). Ces applications n'effacent pas, par ailleurs, tout le contenu des téléphones en cas de saisie (Murray, 2021b; Zagaris et Plachta, 2020).

Le prix des dark phones, et de l'abonnement mensuel payable en cryptomonnaie, peut grandement varier (Regnery, 2020). Phantom Secure offrait ses services pour une somme variant de 335$USD à 500$USD par mois (Pisaric, 2021a). Encrochat vendait ses appareils à l'international au prix d'environ 1,000€ et proposait un abonnement en sus de 250€ par mois pour le service d'assistance disponible 24/7 (Eurojust, 2020). Sky Global offrait ses dark phones à un prix variant de 900€ à 2,000€, en plus d'un abonnement variant de 200€ à 335€ par mois (Pisaric, 2021a). Un coût d'abonnement similaire était exigé pour les dark phones d'Anom (Pisaric, 2021a).

Selon le rapport annuel de 2020/2021 de la New South Wales Crime Commission, les dark phones semblent être devenu un élément central du crime organisé. Bien que ces téléphones aient été créés et commercialisés pour des raisons légitimes au départ, notamment pour une utilisation militaire, plusieurs individus les utilisent afin de commettre des crimes (O'Rourke, 2020; Pisaric, 2021a). Grâce à ces téléphones, les criminels peuvent donc communiquer sécuritairement, afin de gérer leurs activités, telles que le trafic de drogue, le blanchiment d'argent, le trafic humain et même le terrorisme (Barker, 2021; Miller et Bossomaier, 2021). Les dark phones semblent jouer un rôle indispensable dans les opérations des narcotrafiquants particulièrement (Boyer, 2001). Cela témoigne de la capacité d'adaptation des délinquants pour dissimuler leurs activités criminelles (Vincze, 2016). Le nombre d'utilisateurs des dark phones varie d'une compagnie à l'autre. Encrochat comptait environ 60,000 utilisateurs dans le monde, et presque la totalité d'entre eux était impliquée dans des activités criminelles (Eurojust, 2020; Murray, 2021b; Scroxton, 2020). Phantom Secure aurait eu pour sa part 10,000 utilisateurs. Sky ECC aurait eu plus de 170,000 clients et 70,000 dark phones étaient actifs sur le réseau Sky ECC au moment de sa fermeture; les utilisateurs de ces derniers s'échangeraient plus de 3 millions de messages chaque jour. En mai 2021, plus de 11,000 individus provenant de plus de 100 pays avaient acheté un téléphone Anom.

Les enquêtes policières sur les dark phones

Bien que les dark phones soient présentés comme étant à l'épreuve de toute surveillance, incluant celle des forces de l'ordre, ils ne le sont pas nécessairement en réalité (Pisaric, 2021a). Beaucoup de compagnies de dark phones ont été visées par des opérations policières au cours de la dernière décennie. Ces démantèlements réussis montrent que les utilisateurs de ce type de téléphone ne peuvent espérer éternellement opérer en toute impunité. C'est ce que la police néerlandaise a démontré tout d'abord en faisant une enquête sur le propriétaire d'Ennetcom (Ontario Superior Court of Justice, 2016). Cette enquête a mené à une perquisition par la police néerlandaise sur les serveurs de l'entreprise, perquisition autorisée par un juge canadien en 2016, car les serveurs étaient basés au Canada (Ontario Superior Court of Justice, 2016; Pisaric, 2021a). À la suite de cette action, Ennetcom a été mis hors service et des arrestations ont eu lieu, dont celle de son propriétaire (Regnery, 2020). Il y a plusieurs questionnements sur la légalité de l'opération qui ont été soulevés lors des procédures judiciaires, mais le tribunal pénal d'Amsterdam a jugé que les données collectées sur les serveurs d'Ennetcom ont été obtenues légalement et qu'elles sont admissibles comme preuves (Cour d'Amsterdam, 2018).

Phantom Secure a été visé par une opération conjointe des forces de l'ordre de l'Australie, du Canada et des États-Unis (Barker, 2018; Murray, 2021b). Peu de temps après sa fondation en 2008, des narcotrafiquants mexicains possédaient des BlackBerry de Phantom Secure selon les autorités australiennes (Murray, 2021b). Ce n'est seulement qu'en 2014 cependant que les médias australiens ont commencé à parler des dark phones et des entraves que ces derniers apportaient aux enquêtes policières, notamment pour celles de meurtre (Murray, 2021b). En 2017, lors d'une enquête contre le dirigeant de Phantom Secure, des agents infiltrés du FBI l'ont rencontré en se faisant passer pour des narcotrafiquants voulant se procurer des dark phones (Department of Justice, 2019). Les agents ont acheté 10 appareils avec des abonnements au service et ont renouvelé les services 6 mois plus tard (Department of Justice, 2019, 28 mai). Le dirigeant a commis l'erreur d'avouer aux agents infiltrés que Phantom Secure avait été créé spécifiquement pour faciliter le trafic de drogue et c'est en mai 2018 que lui et ses associés, à la suite de perquisitions, ont été arrêtés par les forces de l'ordre et que l'entreprise a été fermée (Murray, 2021a; Murray, 2021b; Department of Justice, 2019). Cinq hommes ont été accusés d'avoir participé au service et à la vente d'appareils chiffrés en lien avec une entreprise criminelle liée au trafic de drogue transnational (Barker, 2018). Le dirigeant a reçu une peine de 9 ans de prison (Murray, 2021a; Murray, 2021b). Contrairement à l'opération contre Encrochat que nous présentons ci-dessous, il n'y a jamais eu de brèche dans le chiffrement de Phantom Secure;

ses utilisateurs ont donc pu passer à des produits concurrents sans crainte d'être arrêtés (Murray, 2021b).

Les autorités françaises ont observé la présence de dark phones d'Encrochat, compagnie néerlandaise, chez des groupes criminels. Les gendarmes ont découvert qu'Encrochat utilisait des serveurs en France, ce qui leur a permis d'amorcer une enquête sur l'entreprise en 2017 (Pisaric, 2021a; Zagaris et Plachta, 2020). En raison, de l'utilisation de plus en plus répandue des dark phones d'Encrochat par les réseaux criminels dans le monde, les autorités françaises ont ouvert un dossier avec la EU Agency for Criminal Justice Cooperation (Eurojust) et les Pays-Bas (Eurojust, 2020). Cela a mené en avril 2020 à une Joint investigation team (JIT) aux Pays-Bas et en France avec la participation d'Europol pour enquêter sur les communications d'Encrochat (Eurojust, 2020). En France, l'opération nommée Emma 95 a monopolisé plus de 60 militaires de la gendarmerie sous la supervision des magistrats de la juridiction interrégionale spécialisée (JIRS) de Lille qui ont surveillé les communications de milliers d'individus (Eurojust, 2020). Aux Pays-Bas, l'opération s'est déroulée sous le nom de Lemont où des centaines de policiers ont également surveillé les communications des criminels avec l'autorisation du juge d'instruction (Eurojust, 2020). Bien que la méthode utilisée par les forces de l'ordre pour accéder aux systèmes d'Encrochat reste encore inconnue du public, l'hypothèse avancée est que la police a réussi à pirater les appareils de l'entreprise soit en installant un logiciel sur les serveurs responsables des mises à jour des dispositifs ou en diffusant un logiciel malveillant sur les dark phones d'Encrochat (Pisaric, 2021a). À la suite du piratage, les enquêteurs ont pu infiltrer le réseau, et donc avoir accès à des millions de messages écrits par les utilisateurs avant que ces derniers ne soient chiffrés et envoyés (Pisaric, 2021b). Les services d'Encrochat ont pris fin le 13 juin 2020, alors que la compagnie a réalisé que sa plateforme était surveillée par la police, et qu'elle ait envoyé un message à tous ses utilisateurs pour les avertir de jeter immédiatement leurs dark phones (Eurojust, 2020). Les opérations policières ont mené à l'arrestation de plus d'une centaine de suspects, au démantèlement de laboratoires de drogues synthétiques, à des saisies de drogues, d'armes à feu, de montres luxueuses, de voitures et d'argent liquide (Eurojust, 2020; Scroxton, 2020).

Les téléphones de Sky Global devenant de plus en plus utilisés dans le monde par des groupes criminels, la police belge a débuté une enquête vers la fin de 2018. En février 2019, les forces de l'ordre de la France et des Pays-Bas se sont jointes à la Belgique pour surveiller les communications des criminels sur ces appareils (Pisaric, 2021a). L'opération, similaire à celle d'Encrochat, a permis d'intercepter les communications chiffrées. Les différentes organisations policières ont collaboré pour trouver un moyen de déchiffrer les données (Pisaric, 2021a). Bien que les enquêteurs belges n'aient pas expliqué comment ils ont réussi à accéder aux messages déchiffrés, l'hypothèse de Sky Global est que les forces policières ont copié puis modifié leur logiciel, pour ensuite le vendre sous le nom de Sky Global (SKY ECC Technologies, 2021). Ces clones des vrais téléphones auraient été modifiés afin de rendre possible la surveillance des utilisateurs, puis vendus à des délinquants. Les utilisateurs auraient ainsi pensé être protégés par la technologie de Sky Global, alors que ce n'était pas le cas. Les messages déchiffrés ont été lus par les policiers et en mars 2021, plusieurs arrestations, saisies et perquisitions ont eu lieu en Belgique et aux Pays-Bas (Pisaric, 2021a).

Les téléphones cryptés d'Anom étaient bien sécurisés, mais chaque message envoyé était également transmis aux enquêteurs de la police (Pisaric, 2021a). Pour mettre en place Anom, le FBI aurait recruté un informateur, en échange d'une réduction de peine. Cet informateur avait dans le passé vendu des dark phones de Phantom Secure et Sky Global. Il possédait donc une bonne réputation dans le monde criminel, et les connaissances afin de développer une technique pour réacheminer les messages chiffrés vers les serveurs de la police. Cet informateur a utilisé ses contacts pour vendre les téléphones Anom (Pisaric, 2021a). L'opération visant les utilisateurs d'Anom a mené à l'arrestation de plus de 800 personnes, à des perquisitions et à des saisies de drogues, armes à feu, voitures de luxe et argent liquide (Pisaric, 2021).

Les dark phones aujourd'hui

Malgré toutes ces opérations policières, les délinquants utilisent toujours aujourd'hui les dark phones. La compagnie Ciphr, basée au Canada, est souvent mentionnée dans les médias comme un fournisseur de téléphones cryptés (Murray, 2021a; Murray, 2021b). Ciphr est présentement le service de dark phone le plus populaire en Australie et a des liens avec des importations de drogue, des saisies de millions de dollars en argent liquide, des enlèvements et de la torture (Murray, 2021a). Les téléphones Ciphr semblent être l'outil de communication utilisé par les membres du Comanchero Motorcycle Club, une bande de motards criminels en Australie (Murray, 2021b). Les autorités suspectent qu'un ancien Comanchero, qui habite aujourd'hui à Dubaï, aurait acheté les droits de distribution de Ciphr pour l'Australie (Murray, 2021a; Murray, 2021b). Une source policière explique qu'au cours de l'année 2020, la majorité des arrestations ou saisies en lien avec le crime organisé impliquait l'utilisation de téléphones Ciphr et qu'aucune entreprise légitime ne semble les utiliser, car d'autres options moins coûteuses et offrant une sécurité similaire existent (Murray, 2021). Les dark phones de Ciphr sont disponibles au coût de 2,500$USD pour un abonnement de 6 mois et le nombre de téléphones Ciphr utilisés dans le monde est estimé à 10,000 (Murray, 2021a; Murray, 2021b). Les dark phones de Ciphr sont des téléphones Samsung ou BlackBerry sans caméra, microphone, port USB et GPS; ils sont vendus avec un logiciel de messagerie chiffrée déjà installé (Murray, 2021a). Ces téléphones ont l'option d'être immédiatement effacés à distance en cas de saisie (Murray, 2021a).

De nouvelles entreprises de dark phones tentent également de faire leur place. Ces compagnies semblent opérer sur un territoire précis, souvent balisé par les frontières nationales. Ainsi, l'Australie (Diamond Secure, NCrypt, Cryptophone Australia, NSI Global Counter Intelligence), le Royaume-Uni (Blackphone, Cipher), les États-Unis (Purism), les Émirats arabes unis (Kryptotel), l'Allemagne (GSMK), la Chine (SYC Secured Smartphone), la France (CryptoFrance), le Canada (Cryptcom) et l'Italie (Endoacustica) ont chacun au moins un fournisseur (Murray, 2021b; Harkin et Molnar, 2022). Les compagnies Armadillo Phone et Wireless Warehouse sont basées au Canada et offrent leurs services à l'international. Toutes ces entreprises se présentent comme offrant des dark phones assurant une sécurité et une confidentialité extrême à leurs utilisateurs. Par exemple, Armadillo Phone , fondé en 2016 et basé au Canada, publicise ses produits sur son site Internet en mentionnant que leurs téléphones offrent une protection contre les pirates informatiques et qu'ils peuvent contourner la surveillance. Les téléphones vendus sont des Google Pixel 3A qui utilisent plusieurs couches de chiffrement pour sécuriser les données, et qui ont l'option de se faire retirer la caméra et le microphone. Il est également possible d'effacer tout

le contenu du dispositif à distance en entrant un mot de passe ou après un délai dans les cas où le téléphone n'est pas déverrouillé. Le téléphone se vend à l'international à un coût variant de 795$USD et 1,445$USD selon la version choisie. Du côté de Wireless Warehouse , les appareils vendus sont des BlackBerry PGP qui fonctionnent à l'aide d'une clé de session qui est transmise au destinataire pour lui permettre de décrypter ses messages. Toutes les données sont stockées sur un serveur canadien et les téléphones se vendent à l'international à un coût variant de 150$CAD à 210$CAD selon le type de téléphone; l'abonnement est de 750$CAD pour 3 mois, 995$CAD pour 6 mois et 1,950$CAD pour 12 mois.

Les défis du chiffrement des téléphones pour les enquêtes policières

L'utilisation d'appareils chiffrés peut apporter certains défis dans les enquêtes policières. En effet, le chiffrement permet de dissimuler les activités des délinquants, et peut aussi empêcher les forces policières d'obtenir les preuves nécessaires à une condamnation, faire échouer l'interception des communications jouant un rôle dans la prévention d'attaques terroristes, ainsi que retarder et augmenter les coûts des enquêtes criminelles (Denning et Baugh, 1999). Dans la majorité des cas qui impliquent un appareil chiffré, il y a un risque élevé que l'enquête ne puisse être menée à terme, car les forces de l'ordre n'arrivent pas à accéder aux données de l'appareil pouvant servir de preuve (Forte, 2009; Vincze, 2016). Ce risque est aussi bien présent dans le cas des téléphones commerciaux vendus par Apple et Samsung par exemple, et qui offrent de chiffrer les données sur les téléphones, mais pas les communications. Selon un rapport du bureau du procureur de Manhattan (2015), dans plus d'une centaine de cas d'analyse de téléphones commerciaux, de septembre 2014 à octobre 2015, les forces de l'ordre n'ont pas été en mesure de perquisitionner les téléphones commerciaux des suspects, car les données des appareils étaient chiffrées. Ces cas concernent des abus sexuels d'enfants, des homicides, du trafic sexuel, des tentatives de meurtre, des voies de fait et des vols. Traditionnellement, les forces de l'ordre utilisaient la méthode d'essais et erreurs pour briser les clés de chiffrement, mais cela pouvait nécessiter des millions de tentatives et prendre plusieurs jours, voire même des mois (Hill-Smith, 2019). Aujourd'hui, les téléphones commerciaux se verrouillent ou sont effacés après une douzaine de tentatives de combinaisons, et donc les attaques par essais et erreurs sont pratiquement impossibles (Hill-Smith, 2019). Cela est d'autant plus vrai pour les dark phones qui limitent encore plus les essais et erreurs de combinaisons. Les autorités ont maintenant recours à des méthodes leur permettant d'exploiter une faille de sécurité inconnue des fabricants leur donnant ainsi la possibilité d'accéder aux données tant et aussi longtemps que le fabricant n'aura pas corrigé la faille (Hill-Smith, 2019).

Le chiffrement, bien que très utile pour protéger la confidentialité des données, rend difficiles l'accès et l'analyse de renseignements qui sont en lien avec des activités criminelles (Ilbiz et Kaunert, 2021). Un exemple de cette problématique a été observé à la suite à l'attaque terroriste de San Bernardino aux États-Unis en 2015, où le Federal Bureau of Investigation (FBI) et la National Security Agency (NSA) n'ont pas été en mesure d'accéder aux données d'un téléphone commercial (iPhone) du terroriste, en raison de son chiffrement par défaut (Ilbiz et Kaunert, 2021; Parikh, Shani, Dave et Patel, 2017). Le FBI a fait une demande à Apple pour pouvoir contourner le chiffrement et accéder à tout le contenu du téléphone (Parikh, Shani, Dave et Patel, 2017). Apple a refusé, pour des raisons de confidentialité, de respect de la vie privée et de confiance des consommateurs (Berthelet, 2018). Le FBI a obtenu une ordonnance émise par un juge fédéral demandant à Apple de contourner leurs fonctions de sécurité pour laisser le FBI accéder aux données chiffrées (Lichtblau et Benner, 2016, 17 février). Ce cas n'est pas le premier où une entreprise a été ordonnée de déchiffrer ses propres données (Lichtblau et Benner, 2016, 17 février). Malgré l'ordonnance, Apple a refusé et comptait faire appel. Le FBI a toutefois renoncé aux poursuites, et plutôt payé la somme de 1.3 million de dollars USD pour obtenir un outil permettant de déchiffrer les données du téléphone commercial (Lichtblau et Benner, 2016; Parikh, Shani, Dave et Patel, 2017). Cet exemple met en lumière les difficultés que le chiffrement apporte aux organisations d'application de la loi dans leurs enquêtes, et ce, dans le cas des téléphones commerciaux. Il est attendu que les compagnies qui fournissent les dark phones, proposent autant sinon moins de coopération aux forces de l'ordre. Selon Woods (2017), les autorités ont au moins deux options pour accéder à des données chiffrées. La première est d'essayer d'obliger le fabricant du dispositif chiffré à désactiver le chiffrement de l'appareil, comme le FBI a tenté de faire avec l'ordonnance imposée à Apple. La deuxième consiste à briser ou à contourner le chiffrement de l'appareil, ce qui peut être difficile et nécessiter certaines compétences techniques. La tendance actuelle amène les grandes entreprises, par souci de respect des protections juridiques et de la confidentialité de leurs utilisateurs, à s'opposer à fournir des informations aux forces de l'ordre en contestant les demandes judiciaires (Boustead, 2020).

Les défis légaux du chiffrement des téléphones

Actuellement, les lois canadiennes permettent aux autorités d'utiliser tous les moyens techniques requis pour déchiffrer des informations qu'elles ont légalement le droit de consulter (Penney et Gibbs, 2017). Cependant, les forces policières n'ont pas toujours les connaissances et les capacités techniques pour le faire. Alors, pour accéder aux données chiffrées de l'appareil d'un suspect, elles ont deux options législatives principales (Penney et Gibbs, 2017). La première consiste à exiger du fournisseur qu'il accorde exceptionnellement l'accès aux données chiffrées à la police. La deuxième consiste à obliger légalement les suspects à déchiffrer leurs données en imposant des sanctions pénales s'ils refusent. Cependant, sachant que les données des dark phones peuvent être effacées à distance, ou suite à certaines manipulations, même si les autorités parviennent à obtenir l'accès au dispositif légalement ou à l'aide de moyens techniques, elles ne pourront pas toujours accéder au contenu supprimé du téléphone (O'Rourke, 2020). Au Canada, l'arrêt Boudreau-Fontaine (2010 QCCA 1108), de la Cour d'appel du Québec, montre qu'en vertu de l'article 7 de la Charte canadienne des droits et libertés sur le droit au silence et le droit à la protection contre l'auto-incrimination, il n'est pas possible d'obliger un individu, que ce soit verbalement ou à l'écrit, à révéler ses mots de passe permettant l'accès aux données chiffrées sur un appareil électronique, tel qu'un ordinateur ou un téléphone mobile. Cela semble également être le cas aux États-Unis selon le cinquième amendement (Terzian, 2016). Cependant, contrairement au Canada, où il ne semble pas y avoir de disposition à cet égard, les lois américaines peuvent forcer un individu à déverrouiller son téléphone protégé par un mot de passe biométrique, tel qu'une empreinte digitale (Ellyson, 2018; Terzian, 2016). Ce problème d'accès au mot de passe s'applique également dans le cas de données chiffrées, car en ayant une clé d'accès, il est

possible de déchiffrer les informations de l'appareil et donc de les consulter (Guarda, 2014).

Dans les prochaines années, selon Guarda (2014), les défis en lien avec l'augmentation des technologies de chiffrement ne seront pas liés aux fouilles, aux perquisitions ou aux saisies, mais plutôt au droit contre l'auto-incrimination de l'article 7 de la Charte. Guarda (2014) explique qu'en raison du paragraphe 11c) de cet article, on ne peut pas exiger d'un accusé qui ne témoigne pas à son procès de fournir l'accès à ses données chiffrées. C'est le cas aussi pour les témoins qui sont protégés par l'article 13. dans R. c. Sonne (2012 ONSC 584). La Cour supérieure de l'Ontario a spécifié que le fait qu'un individu ait recours au chiffrement ne devrait pas être considéré comme quelque chose de pénalisant, car bien que cela puisse servir à dissimuler les preuves d'une activité criminelle, le chiffrement est aussi utile pour empêcher l'accès à des informations confidentielles qui ne sont pas de nature criminelle. De plus, dans le cadre de probations, il est possible d'imposer certaines conditions en lien avec le chiffrement à l'accusé. En effet, dans R. c. Wilson (2014 BCSC 663), l'accusé s'est fait imposer comme condition lors de sa probation de ne pas utiliser de logiciels de chiffrement ou de programmes permettant l'effacement des données d'un appareil. Dans R. c. Duff (2010 ONCJ 493), le juge a exigé de l'accusé qu'il fournisse les clés de déchiffrement de ses appareils à son agent de probation pour permettre leur inspection aléatoire.

Il existe donc une tension opposant la confidentialité à la sécurité dans les décisions des législateurs. Ces derniers se questionnent à savoir si les organismes d'application de la loi devraient avoir accès aux clés de déchiffrement dans les cas où des preuves de commission d'un crime sont présentes (Denning et Baugh, 1999; Hughes, 2002). Certains législateurs proposent de bannir le chiffrement infaillible et d'obliger les compagnies qui créent des dispositifs chiffrés à inclure une clé d'accès, connue du gouvernement, permettant alors aux forces policières de contourner le chiffrement d'appareils lors d'enquêtes (Taylor, 2017). En ce sens, différents projets de loi ont été mis en place à travers le monde afin de faciliter l'accès aux données chiffrées par les autorités. Par exemple, depuis 1994, en réponse à l'émergence des technologies qui rendaient difficile la surveillance électronique, le Communications Assistance for Law Enforcement Act (CALEA) a été adoptée aux États-Unis (Lin, 2018). Cette loi oblige les entreprises à coopérer avec les forces de l'ordre pour les aider à intercepter les communications électroniques. Cependant, le CALEA n'interdit pas l'adoption de certaines fonctionnalités de chiffrement par les fournisseurs et ne donne pas la responsabilité du déchiffrement à l'entreprise en question, sauf si les clés de chiffrement sont encore à la disposition de l'entreprise (Finklea, 2016; Lin, 2018). Depuis son adoption, certaines dispositions du CALEA ont été élargies administrativement, mais aucune proposition législative n'a été adoptée pour le moment (Lin, 2018). De plus, en 2016, aux États-Unis, la règle 41 du Federal Rules of Criminal Procedure a été modifiée pour étendre les pouvoirs du FBI en leur permettant de pirater des ordinateurs, même hors du pays, en obtenant un mandat de n'importe quel juge américain (Khandelwal, 2016). La même année, au Royaume-Uni, l'Investigatory Powers Act a été adopté pour permettre aux autorités d'acquérir et de conserver des données chiffrées pouvant servir de preuves devant le tribunal, ainsi qu'obtenir des pouvoirs leur permettant de contourner secrètement la sécurité cryptographique d'un appareil (Severson, 2016). Au Canada, la partie VI de la Loi sur le SCRS (1984) permet aux autorités canadiennes d'intercepter légalement les communications privées d'un individu, mais il n'est pas garanti que ces communications seront intelligibles ou déchiffrables. West et Forcese (2019) expliquent qu'il n'y a pas officiellement de loi spécifique sur le chiffrement ou d'obligations légales de déchiffrer au Canada. Les forces de l'ordre peuvent donc utiliser divers instruments administratifs plus anciens, tel que le Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications de 2008 qui permet aux autorités, lorsqu'elles ont l'autorisation légale d'accéder aux communications, d'exiger aux fournisseurs d'un appareil de leur fournir la clé de déchiffrement. Cela n'inclut pas le chiffrement qui peut être utilisé à l'insu du fournisseur, par exemple sur un dark phone modifié (SGES, 2008).

Ces lois ont donc comme objectif de permettre aux forces de l'ordre d'accéder aux preuves essentielles afin de condamner les suspects d'un crime (Woods, 2017). Les autorités ne cherchent alors pas à accéder à des données confidentielles, mais plutôt à accéder à des renseignements pertinents pour les enquêtes et pour la sécurité nationale (Woods, 2017). Cependant, plusieurs experts mentionnent qu'il est impossible de concevoir un accès exceptionnel aux données chiffrées d'un appareil pour les forces policières sans compromettre la sécurité des utilisateurs face à des acteurs malveillants (Penney et Gibbs, 2017). En effet, révéler la clé de déchiffrement permettant d'accéder à des données chiffrées peut être problématique. Dans l'affaire R. c. Mirarchi (2015 QCCS 6628), en lien avec une enquête de meurtre par la Gendarmerie royale du Canada (GRC) sur le crime organisé à Montréal, la défense révèle que l'organisation policière avait accès à la clé de déchiffrement intégrée dans tous les appareils BlackBerry de la planète. La Couronne mentionne que les communications déchiffrées par la GRC constituent l'intégralité de la preuve qu'elle a dans ce dossier. Le procureur a invoqué le privilège d'enquête et a expliqué que divulguer la clé de déchiffrage pourrait menacer la vie privée des utilisateurs de BlackBerry mais aurait aussi pour effet de limiter la capacité des autorités à enquêter sur les crimes, ce qui mettrait à risque la sécurité publique. Cependant, le tribunal conclut que la rétention de cette information empêcherait la défense de vérifier l'exactitude des messages déchiffrés et l'identité des correspondants. Il a alors ordonné à la GRC de divulguer la clé de déchiffrement des BlackBerry. La Couronne, ne voulant pas révéler la clé, a donc abandonné les accusations de meurtre contre l'accusé et au cours des deux années suivantes, des accusations contre des dizaines d'individus ayant été arrêtés dans le cadre de la même opération ont également été suspendues pour la même raison (Cherry, 2017). L'affaire Mirarchi met donc en lumière le débat du chiffrement entre le renseignement et la preuve, ainsi que le risque que des moyens techniques soient divulgués au public (West et Forcese, 2019).

Par ailleurs, au Royaume-Uni, l'utilisation d'un dark phone n'est pas criminelle en soi, mais sera plutôt considérée comme un facteur aggravant devant le tribunal quand son utilisation est faite au sein d'un groupe criminel pour planifier un crime et éviter la détection (O'Rourke, 2020). Cela semble être également le cas au Canada, car dans R. c. Boyer (2015 QCCQ 11693) et R. c. Edison (2017 NBBR 102), l'utilisation d'un dark phone, soit un BlackBerry muni d'un système PGP, afin de dissimuler du trafic de stupéfiants, constitue un facteur aggravant dans les deux cas selon le juge. Dans l'opération contre Phantom Secure, les procureurs ont mentionné que les téléphones cryptés ne sont pas accessoires à un crime, comme peuvent l'être les téléphones d'Apple ou Google, mais plutôt que ces téléphones ont été délibérément créés pour aider les activités criminelles (Cox, 2019).

Conclusion

Les dark phones ne représentent qu'une des multiples innovations technologiques qui transforment les activités criminelles. De concert avec le darkweb et les cryptomonnaies, les dark phones représentent un défi important pour les enquêtes policières qui font face à un problème du 'going dark' (ou de darkphone comme dans Regnery, 2020), défini comme la difficulté croissante des services de police à surveiller et collecter de la preuve contre des délinquants (Christie, 2019). De futures études devraient s'intéresser au processus décisionnel qui accompagne l'utilisation des dark phones par les délinquants. Bien que le coût des téléphones rende prohibitive leur utilisation par bien des délinquants, il serait intéressant de comprendre comment et pourquoi des délinquants décident d'utiliser de tels appareils, même si leur fiabilité a été mise à mal à de nombreuses reprises tel que présenté dans cet article. Il serait également intéressant d'interroger les individus qui rendent ces dark phones disponibles pour comprendre leurs motivations, et comment ils arrivent à développer des compagnies plus ou moins légitimes dans ce domaine. Les dark phones ne représentent pas une panacée pour les délinquants, mais ils sont tout de même une innovation technologique au fort impact tant sur le système de justice que sur les enquêtes policières qui méritera d'être étudié au même niveau que le darkweb et les cryptomonnaies.

Financement

Ce document a été financé par la Fondation du Barreau du Québec

Références

Barker, S. (2021). Decrypted: Phantom Secure takedown a 'significant blow' against Australia's organised crime networks Journal of the Australian of Policing Inc. 13 (1), p. 13

Berthelet, P. (2018). Aperçus de la lutte contre la cybercriminalité dans l'Union européenne. Revue de science criminelle et de droit pénal comparé, 1, 59-74. https://doi.org/10.3917/rsc.1801.0059

Boustead, A. E. (2020). The tools at hand: surveillance innovations and the shifting role of federal law enforcement in drug control. Ohio State Journal of Criminal Law, 18(1), 1-24.

Boyer, J. (2001). 16. Commerce et technique au secours du narcotrafic. Dans : J. Boyer, La guerre perdue contre la drogue (pp. 296-315). Paris: La Découverte. https://www.cairn.info/la-guerre-perdue-contre-la-drogue--9782707132864-page-296.htm?contenu=resume

Cents, R., et Le-Khac, N.-A. (2020). Towards a New Approach to Identify WhatsApp Messages. 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 10.1109/TrustCom50675.2020.00259

Cherry, P. (2017, 24 mars). Charges to Be Stayed in Major Montreal Mafia Bust Project Clemenza. Montreal Gazette. https://montrealgazette.com/news/local-news/charges-to-be-stayed-in-major-montreal-mafia-bust-project-clemenza/

Christie, J. (2019). "Going Dark" – The Challenge Facing Law Enforcement in the 21st Century. Economic Crime Forensics Capstones. 45. https://digitalcommons.lasalle.edu/ecf_capstones/45

Cour d'Amsterdam (2018). Jugement No. 13/997097-16, April 19, 2018. https://nl.vlex.com/vid/uitspraak-n-13-997097-764733873

Cox, J. (2017). Dutch Cops Say They've Decrypted PGP Messages On Seized Server. En ligne: https://www.vice.com/en/article/3dyaqk/dutch-cops-say-theyve-decrypted-pgp-messages-on-seized-server

Cox, J. (2019, 22 octobre). Inside the Phone Company Secretly Run By Drug Traffickers.Vice. https://www.vice.com/en/article/wjwbmm/inside-the-phone company-secretly-run-by-drug-traffickers

Denning, D.E. et Baugh, W.E. (1999). HIDING CRIMES IN CYBERSPACE. Information, Communication & Society, 2, 251-276. https://www.semanticscholar.org/paper/HIDING-CRIMES-IN-CYBERSPACE-Denning-Baugh/829b07977c7999572515701fa5d4af197e71df7e

Department of Justice (2019, 28 mai). Chief Executive of Communications Company Sentenced to Prison for Providing Encryption Services and Devices to Criminal Organizations. https://www.justice.gov/usao-sdca/pr/chief-executive-communications-company-sentenced-prison-providing-encryption-services

Diffie, W. et Landau, S. (2010). Privacy on the Line - The Politics of Wiretapping and Encryption. The MIT Press.

Ellyson, L. (2018). Fouilles, saisies et perquisitions de données informatiques : Attente raisonnable de vie privée et infonuagique [mémoire de maîtrise, Université de Montréal]. Papyrus. https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22849/Ellyson_Laura_2018_memoire.pdf

Eurojust (2020, 2 juin). Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.eurojust.europa.eu/dismantling-encrypted-network-sendsshockwaves-through-organised-crime-groups-across-europ

Eurojust (2021, 10 mars). New major interventions to block encrypted communications of criminal networks. https://www.eurojust.europa.eu/news/new-major-interventions-block-encrypted-communications-criminal-networks

Eymard, O. (2018). Questions de cryptologie. Délibérée, 3, 60-63. https://doi.org/10.3917/delib.003.0060

Finklea, K. (2016). Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations, Congressional Research Service. https://nsarchive.gwu.edu/sites/default/files/documents/3996851/CongressionalResearch-Service-Encryption-and.pdf

Forte, D. (2009). Do encrypted disks spell the end of forensics? Computer Fraud and Security, 2009, 18–20.

Graham, R. (2016). How Terrorists Use Encryption. CTC Sentinel. Vol 9 (6), pp. 20-25. https://ctc.westpoint.edu/wp-content/uploads/2016/06/CTC-

Guarda, N. D. (2014). Digital encryption and the freedom of self incrimination: implications for the future of canadian criminal investigations and prosecutions. Criminal Law Quarterly, 61(1), 119-142. https://heinonline.org/HOL/Page?handle=hein.journals/clwqrty61&id=125&collection=journals&index=

Harkin, D. et Molnar, A. (2022). Exploring the social implications of buying and selling cyber security. Crime Law Soc Change. https://doi.org/10.1007/s10611-022-

Hill-Smith, M. (2019). Smartphone Encryption: Legal Framework for Law Enforcement to Survive the «Going Dark» Phenomenon. Auckland University Law Review, 25, 173-198. https://heinonline.org/HOL/Page?handle=hein.journals/auck25&collection=journals&id=173&startid=&endid=198

Hughes, D. M. (2002). The use of new communications and information technologies for sexual exploitation of women and children. Hastings Women's Law Journal, 13(1), 127 146. https://www.researchgate.net/publication/265199999_The_Use_of_New_Communications_and_Information_Technologies_for_Sexual_Exploitation_of_Women_and_Children

Ilbiz, E. et Kaunert, C. (2021): Europol and cybercrime: Europol's sharing decryption platform, Journal of Contemporary European Studies, DOI:10.1080/14782804.2021.1995707

Keenan, B. (2019). State access to encrypted data in the United Kingdom: The 'transparent' approach, Sage Journals. 49(3-4). 223-244. https://doi.org/10.1177%2F1473779519892641

Khandelwal, S. (2016, 1 décembre). Rule 41—FBI Gets Expanded Power to Hack Any Computer in the World, Hacker News. https://thehackernews.com/2016/11/fbi-rule-41-hacking.html

Lichtblau, E. et Benner, K. (2016, 17 février). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. The New York Times. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

Manhattan District Attorney's Office (2015, novembre). Report of the Manhattan disctrict attorney's office on smartphone encryption and public safety. https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf

Miller, S. et Bossomaier, T. (2021). Privacy, Encryption and Counter-Terrorism. Counter-Terrorism, Ethics and Technology, 139-154. https://doi.org/10.1007/978-3-030-90221-6_9

Murray, D. (2021a). Criminals targeted for encrypted phones. Journal of the Australian of Policing Inc. 13 (1), p. 9.

Murray, D. (2021b). Trouble on line for criminals using encrypted phones. Journal of the Australian of Policing Inc. 13 (1), p. 10-11

New South Wales Crime Commission. (2021). Annual Report 2020-21. https://www.crimecommission.nsw.gov.au/files/nsw-crime-commission-

Ontario Superior Court of Justice (2016). Mutual Legal Assistance in Criminal Matters Act (Re), 2016 ONSC 5699 (CanLII). https://www.canlii.org/en/on/onsc/doc/2016/2016onsc

O'Rourke, C. (2020). Is this the end for "encro" phones? Computer Fraud & Security, 2020(11), 8–10. doi:10.1016/s1361-3723(20)30118-4

Parikh, D., Shani, H., Dave, S., Patel, P. (2017) Organized CyberCrime and the State of User Privacy. IJIRST || National Conference on Latest Trends in Networking and Cyber Security.

Penney, S. et Gibbs, D. (2017). Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. McGill Law Journal / Revue de droit de McGill, 63(2), 201–245. https://doi.org/10.7202/1058192ar

Pisaric, M. (2021a). Encrypted mobile phones. Archibald Reiss Days, 11(1). http://eskup.kpu.edu.rs/dar/article/view/293/191

Pisaric, M. (2021b). Mobile phone encryption as an obstacle in criminal investigation – review of comparative solutions. Annals of the Faculty of Law in Belgrade, LXIX (2), 415-442

Public Safety Canada, National Security Technology Division. (2008). Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table. https://cippic.ca/uploads/ATI-SGES_Annotated-2008.pdf

R. c. Boudreau-Fontaine, 2010 QCCA 1108

R. c. Boyer, 2015 QCCQ 11693

R. c. Duff, 2010 ONCJ 493

R. c. Edison, 2017 NBBR 102

R. c. Mirarchi, 2015 QCCS 6628

R. c. Sonne, 2012 ONSC 584

R. c. Wilson, 2014 BCSC 663

Regnery, M. (2020). The dark phones (Encrochat) — Criminals are building their own communication system. En ligne: https://xperylab.medium.com/the-dark-phones-encrochat-criminals-are-building-their-own-communication-system-474f3aeef759

Schneier, B., Seidel, K. et Vijayakumar, S. (2016). A Worldwide Survey of Encryption Products. The Berkman Center for Internet & Society Research Publication Series. Harvard University. https://cyber.law.harvard.edu/publications/2016/encryption_survey

Severson, D. (2016, 14 mars). Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill, Lawfare. https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers

Scroxton, A. (2020). Cops take out encrypted comms to disrupt organised crime. Australia's organised crime networks Journal of the Australian of Policing Inc. 13 (1), p. 27.

SKY ECC Technologies. (2021). SKY ECC platform remains secure and no authorized Sky ECC device has been hacked. En ligne: https://www.globenewswire.com/news-release/2021/03/10/2190026/0/en/SKY-ECC-platform-remains-secure-and-no-authorized-Sky-ECC-device-has-been-hacked.html

Taylor, S. B. (2017). Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark. Science and Technology Law Review, 19(2).https://scholar.smu.edu/scitech/vol19/iss2/6

Terzian, D. (2016). The Micro-Hornbook on the Fifth Amendment and Encryption Georgetown Law Journal. https://ssrn.com/abstract=2725525

Touzin, C., Cameron, D. & Renaud, D. (2015). "Trahi par son BlackBerry, le caïd Raynald Desjardins plaide coupable". En ligne : https://www.lapresse.ca/actualites/justice-et-affaires-criminelles/proces/201507/06/01-4883499-trahi-par-son-blackberry-le-caid-raynald-desjardins-plaide-coupable.php.

US District Court, Southern District California (2021, 17 mai). Application for a warrant by a telephone or other reliable electronic means in Case No. '21 MJ01948. https://storage.courtlistener.com/recap/gov.uscourts.casd.707623/gov.uscourts.casd.707623.1.0.pdf

Vincze, E., A. (2016) Challenges in digital forensics, Police Practice and Research, 17:2, 183-194, DOI: 10.1080/15614263.2015.1128163

Weinstein, J., M. (2015) Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era, American Criminal Law Review, 52(4), 748-49. https://law-journals-books.vlex.com/vid/privacy-vs-public-safety-636937737

West, L. et Forcese, C. (2019). Twisted Into Knots: Canada's Challenges in Lawful Access to Encrypted Communications. Common Law World Review, 49(3-4), 182–198. http://dx.doi.org/10.2139/ssrn.3443533

Woods, A., K. (2017). Encryption Substitutes, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1705. https://lawfareblog.com/encryption-substitutes

Zagaris, B., & Plachta, M. (2020). Transnational organized crime. International Enforcement Law Reporter, 36(7), 248-255.