ENQUÊTE

L'argument d'un réseau à 100 % criminel est-il bidon ?

Les 170.000 utilisateurs du téléphone crypté Sky ECC étaient-ils vraiment tous des criminels ? Plusieurs éléments troublants sèment le doute sur la légitimité de l'argumentaire des autorités judiciaires pour justifier la surveillance de masse.

PHILIPPE LALOUX

Dans la nuit du 5 au 6 juin 2013, le journal britannique *The Guardian* publiait ce qui, aujourd'hui encore, constitue la plus importante fuite de l'histoire des services de renseignements américains. Plus d'1,7 million de documents secrets archivés dans les serveurs de la National Security Agency (NSA) étaient balancés par le lanceur d'alerte américain, ancien agent de la CIA, Edward Snowden. Le monde découvrait alors comment les autorités américaines et britanniques avaient mis au point une sorte de gigantesque aspirateur de données numériques, lesquelles, après avoir été stockées, décortiquées, triées, leur permettaient d'espionner le monde entier. Et d'extraire les informations utiles pour mener leurs enquêtes. Pour la justice américaine, pas de doute : le programme Prism de la NSA relevait bel et bien de la surveillance de masse généralisée, contraire à la Constitution.

L'affaire Snowden a servi de détonateur à la conception du service de messagerie réputé inviolable, Sky ECC. Pour son fondateur, le Canadien Jean-François Eap, la vie privée en ligne est une vertu cardinale. Pour les autorités judiciaires, en revanche, c'est le début du cauchemar.

« Oui, le cryptage de bout en bout est un vrai problème. Nous serons aveugles si nous ne trouvons pas une solution pour accéder aux données criminelles sur les plateformes de communication », confirme Catherine De Bolle, l'ex-patronne de la police fédérale belge désormais à la tête d'Europol. Or, selon un document publié le 10 février 2023 par le Conseil de l'Union européenne, « les preuves électroniques sont nécessaires dans 85 % des enquêtes concernant des crimes sérieux ».

Où se niche cette mine d'or de données occultes échangées par les narcotrafiquants, les marchands d'armes, les réseaux de blanchiment d'argent ou de traite d'êtres humains ? Sur ces fameuses applications de messageries cryptées de bout en bout, dont seuls l'émetteur ou le récepteur disposent des clés pour déchiffrer les messages. Pour y accéder, pas le choix : il faut pirater la communication en y entrant par une porte dérobée, comme le font les «hackers ».

C'est précisément ce qu'ont fait les forces de police européennes pour intercepter plus d'un milliard de messages sur Sky ECC. Et avant cela déjà, en 2020, sur la messagerie néerlandaise EncroChat. A chaque fois, ces surveillances massives ont débouché sur des coups de filet historiques, affolant tous les compteurs en termes de performances : des centaines de perquisitions, des milliers de tonnes de cocaïne saisies, des dizaines de condamnations… Des trophées de chasse inespérés permettant de justifier un narratif extrêmement bien huilé affirmant avec force que ces outils sont utilisés exclusivement par des criminels. « Nous avons constaté que tous ceux qui possédaient un téléphone Sky ECC étaient des criminels », soutient Catherine De Bolle. « Avec Sky ECC, nous avons également découvert que les criminels se sentaient vraiment intouchables. (…) C'était comme si nous étions à table avec les criminels. Et c'était vraiment le cas, ils discutaient entre eux. Et nous écoutions. »

Oui, le cryptage de bout en bout est un vrai problème. Nous serons aveugles si nous ne trouvons pas une solution pour accéder aux données criminelles sur les plateformes de communication

Catherine De Bolle
Ex-patronne de la police fédérale belge, désormais à la tête d'Europol

Une base fragile

Que des criminels ? C'est toute la question. Autant les dossiers criminels issus des perquisitions ont été solides, autant la légitimité des interceptions massives (donc, sans cibler des suspects en particulier sur base d'un mandat) semble être fragile.

« Nous sommes convaincus que tout ce que nous avons fait était légal. En effet, nous avons bénéficié d'un contrôle judiciaire dès le début de l'affaire », affirme la patronne d'Europol. Or, déjà dans le cas du démantèlement d'EncroChat, plusieurs requêtes en nullité ont dénoncé l'illégalité de la collecte massive de données issues de la messagerie cryptée.

Sky ECC, à la différence d'EncroChat, avait pignon sur rue, que ce soit via le site de Sky ECC, ou à travers un vaste réseau de distributeurs (des boutiques de GSM, en somme). Il se positionne sur un marché que les experts qualifient de « gris », susceptible de toucher tant des utilisateurs légitimes que des criminels. En 2020, ils étaient 170.000, tout confondus. « Honnêtement, nous avons de tout, des prostituées aux journalistes, en passant par les espions et les cadres d'entreprise », affirme l'un des distributeurs, dans un échange versé à la procédure judiciaire. On y retrouve même un ancien formateur du FBI, Robbie Cressman, qui affirme l'avoir utilisé pour des raisons professionnelles et privées.

La thèse de la présomption de culpabilité généralisée défendue par les autorités judiciaires belges va néanmoins convaincre leurs voisins français. « Il est établi par les autorités belges que l'utilisation de la solution Sky ECC sert exclusivement pour faciliter des activités criminelles », écrivent les enquêteurs dans un document dont le consortium de journalistes a pu prendre connaissance. Sur cette base, Jean-François Eap, considéré comme le cerveau d'une organisation criminelle, s'est donc vu inculpé pour avoir facilité des activités criminelles.

Pour autant, le fondateur de Sky ECC n'a pas été entendu par la Justice et n'a

Chat Control, Going Dark… Les plans de l'UE pour surveiller nos messages privés sur WhatsApp ou Signal

Partout en Europe, de la Commission aux Etats membres, les planètes s'alignent. © AFP.

PH.L.

Nous voulons une *front door*, pas une *backdoor*. » En clair : une porte d'entrée légitime, pas une porte dérobée (comme ce fut le cas pour le piratage de Sky ECC par les forces de police), pour mettre sur écoute les messageries privées, réputées inviolables. Le message de Catherine De Bolle, la patronne d'Europol est clair. Le chiffrement de bout en bout de ces messageries, y compris WhatsApp et Signal, est devenu l'ennemi public numéro 1 des autorités judiciaires, particulièrement sous pression depuis les attentats terroristes de 2015. Le succès du démantèlement d'EncroChat et de Sky ECC leur donne un argument providentiel pour placer un mouchard dans nos communications privées. Au nom de la sécurité.

En filigrane, c'est donc bel et bien la vie privée en ligne qui est dans le collimateur. Face au Parlement, le 19 mars dernier, Ine Van Wymersch, la commissaire nationale à la lutte contre la drogue, ne disait pas autre chose : « Voulons-nous, sous la pression de la protection de la vie privée, maintenir l'anonymat des criminels ou rétablir l'équilibre ? Nous devons redonner à la police et à la justice les moyens de traquer les organisations. »

Message reçu. Partout en Europe, de la Commission aux Etats membres, les planètes s'alignent. Y compris en Belgique où quatre ministres (Annelies Verlinden, Vincent Van Quickenborne, Petra De Sutter et Ludivine Dedonder) ont fait passer un projet de loi sur la conservation des données privées de télécommunication (téléphone, inter-