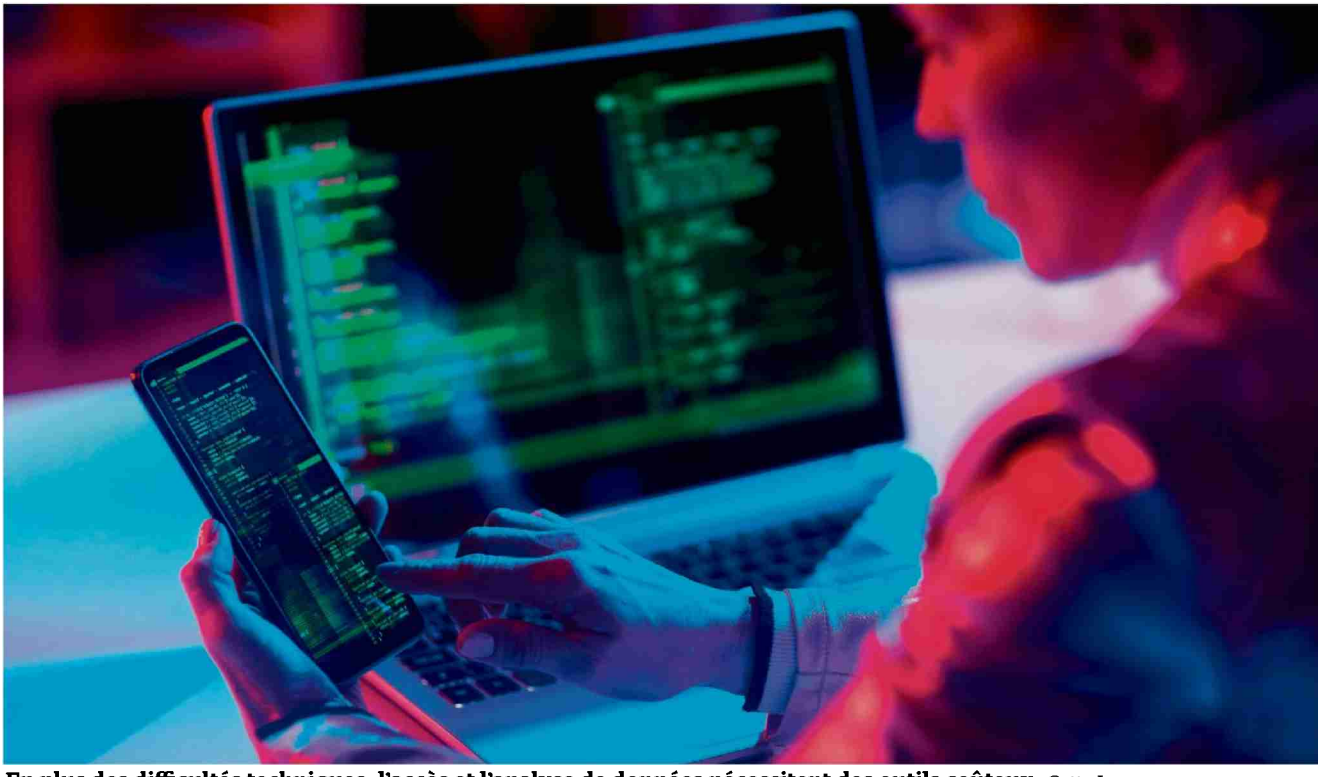
La justice peine à pénétrer les smartphones



En plus des difficultés techniques, l'accès et l'analyse de données nécessitent des outils coûteux. *Getty Images*

INVESTIGATIONS Craquer un téléphone verrouillé serait un jeu d'enfant, si l'on en croit les séries policières. L'enquête sur l'agression d'Annecy montre une tout autre réalité.

DAVID GENILLARD

Le téléphone de l'agresseur d'Annecy révèlera-t-il des secrets sur les prémices de l'attaque au couteau du 8 juin? Il faudra encore patienter pour le savoir. Selon plusieurs médias français, le trentenaire d'origine syrienne a jusqu'ici refusé de communiquer aux enquêteurs le code d'accès de son iPhone. À ce jour, le contenu de l'appareil n'a donc pu être exploré. À l'heure où les cas de cyberattaques en série font les gros titres – la Confédération peut en attester –, les difficultés que rencontrent les autorités françaises pour «entrer» dans le téléphone d'Abdelmessih H. semblent paradoxales. Le smartphone serait-il, contrairement aux idées reçues, un coffre-fort?

En Suisse, la plupart des corps de police disposent des outils nécessaires pour le percer, à l'image de la police cantonale bernoise qui, par la voix de sa porte-parole Isabelle Wüthrich, indique: «Nous avons certaines possibilités de débloquer les portables protégés par des codes de verrouillage. Pour des raisons tactiques, nous ne donnons toutefois pas d'informations plus détaillées à ce sujet.»

Créé en 2010 au sein de l'Institut de lutte contre la criminalité économique (ILCE) de la Haute École de gestion Arc, à Neuchâtel, le Centre d'investigation numérique et de cryptologie accompagne les autorités pour les former à ces technologies. «Technique-

ment, craquer un téléphone portable sans en avoir l'accès peut clairement être difficile, selon le modèle concerné, répond Olivier Beaudet-Labrecque, professeur à l'ILCE. Il faut des outils spécifiques pour y arriver.» Dans le domaine, la société israélienne Cellebrite avec sa série de produits UFED (pour Universal Forensic Extraction Device) fait figure de leader mondial. De l'extérieur, l'engin ne paie pas de mine. «Il s'agit d'une simple mallette avec, à l'intérieur, une tablette, décrit Olivier Beaudet-Labrecque. À une extrémité, on branche l'appareil qu'on cherche à explorer et, à l'autre, un support de données de destination, comme un disque dur.» Le téléchargement des informations prend de quelques minutes à quelques heures.

Un coup de retard

Rien de bien sorcier, à première vue. Sauf que l'univers du smartphone est en constante mutation. «Lorsqu'un nouveau téléphone arrive sur le marché, les sociétés spécialisées dans l'exploitation des données vont commencer par l'examiner pour trouver une façon d'y accéder», poursuit le professeur de l'ILCE. «On cherche des vulnérabilités, soit dans le matériel, soit dans le système d'exploitation, qui permettent d'y parvenir», ajoute Sylvain Pasini, professeur à l'Institut des technologies de l'information et de la communication à la HEIG-VD, à Yverdon.

Durant cette phase d'exploration, les solutions pour craquer l'appareil en question n'existent pas. Les autorités ont donc un coup de retard et le combler demande de gros moyens financiers. «Il y a très peu d'acteurs sur ce marché et la demande est gigantesque: tous les pays, et pas seulement les plus développés économiquement, ont besoin de ces outils, explique Olivier Beaudet-Labrecque. Le coût de ces outils est donc très élevé.» À la Police bernoise, on confirme que «le déblocage mais aussi l'analyse des téléphones portables sont généralement coûteux en moyens».

Jeu de bluff

Dans les salles d'audition, une partie de poker menteur peut donc régulièrement s'engager. «Les enquêteurs vont demander à un prévenu de déverrouiller son téléphone, en expliquant qu'ils y arriveront de toute façon par eux-mêmes en peu de temps, témoigne Me Loïc Parein. On peut se demander parfois si ce n'est pas du bluff.» Autre cas de figure rencontré par Olivier Beaudet-Labrecque: «Il est déjà arrivé qu'un procureur fasse durer l'instruction en attendant que la solution de craquage soit disponible.»

D'autres stratégies permettent d'accéder au contenu d'un appareil électronique sans avoir à le déverrouiller, signale Sylvain Pasini. «Plutôt que de cibler le téléphone, on peut chercher à accéder aux données qui seraient sauvegardées dans le cloud ou sur la carte SD de l'appareil. Par exemple, il existe des sauvegardes WhatsApp qui sont en général protégées par l'application.» La démarche fait furieusement penser aux activités des pirates informatiques. Il ajoute: «En tant que chercheur, c'est vrai qu'il y a un côté parfois schizophrène: mon but est de sécuriser au maximum les données des utilisateurs, mais lorsque nous collaborons avec la police, on tente au contraire d'y accéder en contournant ces mécanismes.»

L'autorité judiciaire dispose toutefois de mesures de contrainte qui permettent de passer outre. «Le procureur peut séquestrer le téléphone et ordonner sa perquisition, détaille Ludovic Tirelli, avocat veveysan spécialisé en droit pénal et nouvelles technologies. Le prévenu peut alors demander la mise sous scellés de son appareil, en invoquant le fait qu'il contient des données sensibles ou couvertes par un secret - typiquement les échanges avec son avocat.» Pour y accéder, le Ministère public doit alors déposer une demande de levée des scellés auprès d'un tribunal des mesures de contrainte. Une procédure qui peut prendre du temps: le juge doit examiner le contenu des données pour déterminer lesquelles sont protégées par le sceau du secret, et lesquelles sont effectivement pertinentes dans le cadre de l'enquête.

La mort du mot de passe

Les smartphones évoluent et les moyens de verrouillage avec eux. Le PIN appartien-

dra bientôt au passé, au profit de la recon-

«Techniquement, craquer un téléphone portable sans en avoir l'accès peut clairement être difficile.»

Olivier Beaudet-Labrecque, professeur à l'Institut de lutte contre la criminalité économique

naissance faciale ou de l'identification par empreinte digitale. Me Parein y voit un dilemme épineux. «La question est de savoir si les enquêteurs pourront exploiter ces moyens de verrouillage. Imaginons le cas d'un prévenu qui refuse de déverrouiller son téléphone. Le policier peut-il alors le brandir devant le visage de son propriétaire lors de l'audition pour accéder au contenu? On peut en douter.»

Peut-on également imaginer exploiter les empreintes digitales prélevées au moment de l'arrestation dans le même but? «Des chercheurs sont parvenus à déverrouiller des téléphones avec des répliques d'empreintes digitales, répond Olivier Beaudet-Labrecque. Mais il y a un grand écart entre ce que l'on peut réaliser en laboratoire avec des conditions optimales et un sujet volontaire et dans la vraie vie. Pour ce qui est de la reconnaissance faciale, la photo ne fonctionne pas et les tests de modélisation 3D de visage ne sont, à ma connaissance, pas concluants.»

«Il y a un côté parfois schizophrène: mon but est de sécuriser les données des utilisateurs, mais lorsque nous collaborons avec la police, on tente de contourner ces mécanismes.»

Sylvain Pasini, professeur à la HEIG-VD

Comment protéger ses données

L'enquête sur l'agresseur d'Annecy en témoigne: il n'est pas si simple d'accéder aux données renfermées dans un smartphone... pour autant que son propriétaire ait les bons réflexes. Pour Olivier Beaudet-Labrecque, de la Haute École de gestion Arc, à Neuchâtel, il faut notamment «effectuer religieusement les mises à jour des applications et du système d'exploitation, être prudent quant aux applications téléchargées et ne se fier qu'aux développeurs et magasins d'applications fiables». Le professeur invite également à se méfier des réseaux wi-fi publics non sécurisés et à rester vigilant face aux messages frauduleux qui peuvent arriver par e-mail, SMS ou sur toute autre application de communication.

Réputés plus difficiles à craquer, l'iPhone et son système d'exploitation iOS devraient-ils être privilégiés face à Android? «Les deux ont des avantages et des inconvénients, répond Sylvain Pasini, de la HEIG-VD. Android est moins restrictif en termes de droits d'accès à d'autres services du téléphone. Lorsqu'on télécharge une nouvelle application, il n'est pas rare qu'un message demande une autorisation pour accéder à la galerie, aux contacts ou à l'appareil photo. Il faut bien se demander si l'application en question en a vraiment besoin avant de cliquer sur «OK.»

Quelques centaines de francs suffisent

Neuf cent mille dollars. C'est la somme que déboursait le FBI en 2016 pour accéder au contenu de l'iPhone 5C de l'un des auteurs de la tuerie de San Bernardino, en Californie. Selon le magazine «Forbes», il en coûterait aujourd'hui plutôt 6000 pour s'offrir un UFED, le plus répandu des systèmes fournis par Cellebrite.

Alors que ses appareils sont destinés aux forces de l'ordre et à la justice, l'entreprise israélienne, leader mondial sur ce créneau, fait face à un marché noir inquiétant. Pour quelques centaines de francs, on peut s'offrir un UFED sur eBay. Il y a quatre ans déjà, Cellebrite enjoignait à ses clients de lui retourner les appareils usagés plutôt que de les revendre, soulignant l'importance des données potentiellement contenues dans ces systèmes. Plusieurs d'entre eux sont à ce jour encore disponibles sur eBay.

Sur son site, l'entreprise affiche des règles éthiques strictes. Elle a constitué un comité qui veille à leur application, s'appuyant sur des spécialistes externes des droits humains. Ce comité examine en continu l'évolution des régimes politiques dans le monde ou celle des lois portant sur la protection des données, et ses clients doivent avoir reçu l'aval de leur gouvernement.

Cellebrite n'en fait pas moins l'objet de vives critiques. Parmi ses détracteurs les plus virulents, Moxie Marlinspike, fondateur de la messagerie Signal, qui a accusé ouvertement l'entreprise d'avoir collaboré avec des régimes autoritaires, parmi lesquels la Russie, la Biélorussie ou encore le Venezuela. La société aurait par ailleurs été victime de cyberattaques, qui auraient conduit à la fuite de 900 GB d'informations.