TECHNOLOGIES

Vie de famille, relation aux autres, environnement... Chaque mardi, « Le Soir » décrypte comment et pourquoi le smartphone a bousculé notre quotidien. Et quel sera son futur ? Aujourd'hui, zoom sur les applications.

« Etre victime de cybersurveillance, c'est être victime d'une arme militaire »

Les logiciels espions sont une menace pour la démocratie, préviennent Sandrine Rigaud et Laurent Richard. A la tête du consortium Forbidden Stories, ils ont enquêté pendant un an avec des dizaines de journalistes internationaux sur ces outils de surveillance. Dans leur livre, ils racontent les coulisses de cette investigation.

ENTRETIEN

JOËL MATRICHE

En juillet 2021, sous la coordination du consortium de journalistes Forbidden Stories et avec l'appui technique du Security Lab d'Amnesty International, seize médias, dont *Le Soir* et *Knack* en Belgique, révélaient comment des Etats ont infiltré les téléphones d'opposants, de journalistes, d'avocats, de militants des droits de l'homme grâce à un logiciel-espion de facture israélienne, Pegasus. Dans *Pegasus, démocraties sous surveillance*, Laurent Richard, fondateur et directeur de Forbidden Stories, ainsi que Sandrine Rigaud, rédactrice en chef, racontent les coulisses de cette enquête transnationale.

Plus de 80 journalistes ont collaboré au Projet Pegasus. Comment cette enquête a-t-elle débuté et combien de temps a-t-elle duré ?

Sandrine Rigaud Il s'est passé environ un an entre la réception des données et la publication. Tout a commencé lorsque, avec Amnesty, nous avons reçu une liste de 50.000 numéros de téléphone dont on savait seulement qu'ils avaient été sélectionnés pour être potentiellement ciblés par Pegasus, un logiciel de surveillance développé et commercialisé par la société israélienne NSO. En tant que journalistes, on a vite compris qu'on était assis sur un scoop mais tout restait à faire, à commencer par savoir à qui appartenaient ces numéros de téléphone. On a d'abord croisé nos propres carnets d'adresses avec cette liste et c'est à ce moment-là, par exemple, que Laurent découvre que le numéro de la journaliste Khadija Ismayilova, avec qui il avait déjà travaillé en Azerbaïdjan, s'y trouve. Il y a aussi le numéro d'un journaliste mexicain avec qui on travaille, Jorge Carrasco, de Proceso… Ça montre alors que dans la liste de NSO, il y a des journalistes – on va en découvrir des dizaines – mais aussi des militants des droits humains, des avocats… Une fois qu'on a identifié quelques centaines de noms, il a fallu analyser les téléphones pour y trouver des traces d'infection par Pegasus, un travail mené avec le Security Lab d'Amnesty. Et puis très vite, vu l'aspect tentaculaire, on a mis en place une équipe internationale. Ce qui, en soi, était déjà compliqué, car on travaillait sur la cybersurveillance et on risquait d'être ciblés nous-mêmes. Il fallait être très prudents, nous déplacer pour voir les gens plutôt que les appeler, mettre en place un nouveau système de communication… Et puis, a débuté une enquête de plusieurs mois avec ces partenaires pour tenter d'identifier d'autres victimes et surtout, analyser le contenu de leurs téléphones pour savoir à quoi et à qui on avait affaire. On a ainsi identifié des histoires très fortes et on a publié.

Il fallait être très prudents, nous déplacer pour voir les gens plutôt que les appeler

David Vincenzetti, cofondateur et directeur de Hacking Team, une autre entreprise de cybersurveillance, disait, c'est repris dans votre livre, que la vie privée est moins importante que la sécurité nationale. Qu'en pensez-vous ?

Laurent Richard C'est l'argument brandi par de nombreux Etats qui surveillent leur population et par les entreprises du secteur : la sécurité nationale passe avant, même avant les libertés fondamentales. Le problème est que le concept de sécurité nationale est extrêmement flou, on ne sait pas de quoi on parle. De quoi parle-t-on quand on retrouve des journalistes, des opposants politiques sur une liste de clients d'un logiciel qui a normalement pour mission d'intercepter les communications de terroristes, de pédophiles, de criminels… ? Ce concept de sécurité nationale, précisément parce qu'il est flou et fourre-tout, permet à des gouvernements de justifier la mise sous surveillance de personnes qui ont en commun de mettre en danger ces pouvoirs, des intérêts puissants dans ces pays. Que ce soient les autorités mexicaines, des cartels, des autocrates qui ont trouvé là le moyen d'exporter la terreur au-delà des frontières.

N'y a-t-il pas la crainte aussi que ces outils, utilisés par des Etats démocratiques ou non, le soient un jour par des groupements privés ou même des entreprises ?

L.R. Sans être dramatico-pessimiste, les choses ne peuvent que s'aggraver tant qu'il n'y a aucune loi, aucune directive, aucun dispositif légal pour nous protéger de cette contagion. Il n'y a personne pour contrôler qui nous surveille, personne pour empêcher qu'un journaliste ou un opposant politique soit sur cette liste. Et il n'y a personne non plus pour vraiment réguler ce marché. On ne parle ici que de NSO mais il y a des dizaines et des dizaines d'entreprises dans le domaine de la cybersurveillance.

La vie d'une personne qui a été surveillée par Pegasus est détruite

S.R. Quand Laurent dit qu'on est dans le pire, on a aussi pu le constater dans une enquête qu'on a menée après Pegasus et qui s'appelle Story Killers. Elle montre comment, aujourd'hui, des officines privées qui n'ont même pas d'existence légale peuvent acquérir des outils de surveillance pour ensuite proposer, que ce soit à des Etats ou à des privés, à des criminels, des hommes politiques corrompus, des solutions clef en main avec non seulement des outils de cybersurveillance mais aussi une gamme complète de désinformation. Ça fait aussi partie de cet arsenal qui fragilise nos démocraties.

Toute nouvelle technologie n'est pas promise au meilleur comme au pire ?

L.R. C'est toujours le même questionnement lorsqu'il y a une avancée scientifique, un progrès technologique. L'intelligence artificielle est capable du pire comme du meilleur, il en va de même des logiciels de surveillance. C'est là qu'entre en jeu le politique, on espère que ce livre va aussi permettre au débat politique d'exister et qu'on pourra bâtir des lois pour nous protéger de ça. On aurait tort de croire qu'il n'y a que les autocrates et les dictatures qui utilisent ce type de logiciel puisque c'est le cas aussi dans pas mal de pays de l'Union européenne. Même si c'est dans un cadre plus strict qu'en Arabie saoudite ou en Azerbaïdjan. Il faut absolument que les gens comprennent à quel point être victime de cybersurveillance, c'est être la victime d'une arme militaire, il y a donc un vrai danger pour nos démocraties. Il faut aussi réaliser à quel point il est traumatisant d'être ciblé par un tel outil. On décrit dans le livre l'expérience de Khadija Ismayilova, journaliste en Azerbaïdjan : elle sait ce que c'est d'être surveillée, elle avait été, en 2012, filmée par des caméras de surveillance planquées dans son appartement et dix ans plus tard, elle est surveillée par Pegasus. Pour elle, c'est pire parce que les dommages collatéraux causés par Pegasus sont immenses, toute personne qui l'a approchée, à qui elle a parlé, a été surveillée aussi. La vie d'une personne qui a été surveillée par Pegasus est détruite car elle sait que ses ennemis détiennent des secrets sur elle et que ces secrets, son intimité peuvent un jour être exposés à la vue de tous. Au niveau européen, il y a eu une commission parlementaire sur Pegasus, la Commission européenne a émis des recommandations mais celles-ci n'ont absolument pas eu d'effet. Au nom de la sécurité nationale, tout débat est écarté.

S.R. Pour apporter une petite note d'optimisme quand même, la réponse politique sera de fait très longue, très compliquée mais certaines entreprises technologiques réagissent car elles sont directement impactées. Juste après la publication du Projet Pegasus, Apple a porté plainte contre NSO et notifie les victimes, ce qui a permis de découvrir de nouveaux abus. C'est bien sûr l'intérêt commercial qui motive ces entreprises mais il va au moins dans l'intérêt du consommateur, qui est un citoyen.