SURVEILLANCE ÉLECTRONIQUE

« Un conseil : soyez parano, plus rien, plus personne n'est à l'abri »

Philippe Hensmans est directeur de la section belge francophone d'Amnesty International. Il appelle à repenser radicalement notre attitude face à un monde en mutation rapide

ENTRETIEN
JOËL MATRICHE

L'ONG, qui a déjà mis en garde à de nombreuses reprises contre l'usage illégitime de logiciels espions, notamment Pegasus, vient de publier un rapport « La pointe de l'iceberg : la crise de la surveillance électronique que provoquent les Etats et les entreprises privées ».

Philippe Hensmans, quelle est votre réaction à la lecture de l'enquête Pegasus que viennent de publier une série de médias et à laquelle a participé le laboratoire d'Amnesty ?
Je ne peux qu'être satisfait. On savait que ces outils existaient, on avait parlé de la société NSO et de son logiciel espion Pegasus dans plusieurs rapports mais sans savoir qui exactement était ciblé par cette surveillance. On sait maintenant que plus rien, plus personne n'est à l'abri. Que des activistes, des journalistes peuvent se faire dérober leurs données et voir celles-ci tomber aux mains des gouvernements. Pour des sujets aussi importants, faire paraître des communiqués de presse ne suffit pas, l'ampleur est tout autre quand des médias arrivent avec une liste de 50.000 numéros de téléphone. Ça a un autre poids.

Votre rapport titre sur « la pointe de l'iceberg ». Que voulez-vous dire ?
Simplement qu'il y a d'autres systèmes que Pegasus qui existent et qui mettent le cyber-espionnage à la porte de n'importe quel Etat.

> *Nous proposons plusieurs pistes dans notre rapport. Notamment un moratoire sur la vente, le transfert et l'usage de ces technologies*

Le Security Lab d'Amnesty a apporté son expertise technique à cette enquête…
Il a été lancé en 2019 à Berlin afin d'enquêter sur les cyberattaques contre la société civile. Cette expertise technologique est au cœur de ce que nous sommes en tant qu'organisation de défense des droits humains. Nous devons tous repenser radicalement la manière dont nous relevons les défis posés par un monde en mutation rapide. Alors que les développements technologiques se poursuivent à un rythme exponentiel, nous devons veiller à ce que ces avancées ne portent pas atteinte à nos droits fondamentaux. Le projet Pegasus a montré comment les attaques numériques contre les militants sont répandues, bien orchestrées et constituent une réelle menace pour nos droits humains.

Quelles solutions apporter à ce que vous qualifiez de « crise mondiale des droits humains » ?
Nous proposons plusieurs pistes dans notre rapport. Notamment un moratoire sur la vente, le transfert et l'usage de ces technologies. Le temps qu'un cadre légal et des instances de régulations soient mis en place. Il faudrait aussi qu'une instance indépendante, qui pourrait par exemple relever des Nations Unies, puisse enquêter sur les cas de surveillance illégale qui ont été cités dans le Projet Pegasus et s'il le faut, que les coupables soient poursuivis et les victimes prises en compte. Il faut aussi que l'on sache à qui ont été accordées des licences pour l'exportation de produits comme Pegasus et surtout, vers quels Etats. Puis que soient révoquées les licences lorsqu'il y a un risque flagrant de violation des droits humains. Il faut surtout accroître la transparence : sur les sociétés actives dans ce secteur, leurs produits, les exportations, etc.

Quel conseil donner aux activistes, aux militants, aux journalistes qui pourraient ainsi être espionnés ?
Qu'ils soient paranos ! Qu'ils se méfient de leurs téléphones. Il y a aussi tout un travail de sensibilisation et de formation à mener sur le terrain.

Le rapport : www.amnesty.be/IMG/pdf/20210723_rapport_pegasus.pdf

Philippe Hensmans : « les attaques numériques constituent une réelle menace pour nos droits humains ». © BELGA.

Plusieurs pays ouvrent des enquêtes sur Pegasus

Depuis dimanche soir et durant toute la semaine, un consortium de 16 médias internationaux – dont *Le Soir* – rassemblés autour de Forbidden Stories a publié, avec l'appui d'Amnesty International, l'enquête intitulée « Projet Pegasus ». Elle révèle comment certains gouvernements ou services secrets ont utilisé le logiciel Pegasus pour la surveillance de journalistes, de politiques ou de défenseurs des droits de l'homme, en se faufilant dans leur téléphone. Ces révélations ont suscité des réactions aux quatre coins du globe. Dans certains pays, la justice s'en mêle. Petit tour d'horizon, non exhaustif.

A.K. (st.)

En France
Suite aux révélations du Projet Pegasus, Emmanuel Macron a convoqué un conseil de défense exceptionnel ce jeudi. Un des numéros du président figurait sur la liste de cibles potentielles du logiciel espion. « Des investigations sont lancées », a assuré le porte-parole du gouvernement sur France Inter. Les téléphones de Lénaïg Bredoux et Edwy Plenel, journalistes à Mediapart, ont été infectés par ce logiciel en 2019 et 2020. Le journal a porté plainte auprès du procureur de Paris. Dans la liste des espionnés, l'ex-journaliste du *Canard enchaîné* Dominique Simonnot a également fait savoir qu'elle saisirait la justice, comme le journal satirique. Le parquet de Paris a ouvert une enquête, notamment pour « accès frauduleux à des systèmes technologiques ».

En Hongrie
Près de 300 numéros de téléphone ont été ciblés par la Hongrie, dont celui de Zoltan Varga, grand patron du Central Media Group (groupe de médias indépendants). L'homme d'affaires avait organisé chez lui, en juin 2018, un dîner avec plusieurs convives. Quelque temps après, les numéros des personnes présentes étaient sur la liste cible de Pegasus. Plusieurs journalistes indépendants ont également été ciblés. Bien que le Security Lab d'Amnesty International ait trouvé des traces du logiciel dans plusieurs téléphones, la Hongrie réfute toutes les accusations. Le parquet de Budapest a toutefois annoncé l'ouverture d'une enquête « sur le recueillement potentiel non autorisé d'informations confidentielles ».

Au Mexique
Ce sont carrément des proches et la famille de M. Lopez Obrador, le président actuel du pays, qui auraient été ciblés par le logiciel espion lorsque celui-ci était à la tête de l'opposition au président Pena Nieto. Mais il y a également des journalistes, des avocats, des hommes et femmes politiques, etc., qui ont été pris pour cibles. Marcela Turati, une journaliste indépendante, est certaine d'avoir été victime du logiciel. « Je pense que presque tous les journalistes au Mexique savent et sentent qu'ils sont soumis à une sorte de surveillance car le Mexique est l'un des pays les plus dangereux pour exercer notre profession », a-t-elle affirmé à l'AFP, lundi. Une enquête a été ouverte par la justice mexicaine au sein du gouvernement.

En Israël
Le pays, mondialement reconnu pour ses compétences en cybersécurité, héberge le siège de NSO (la société qui a développé Pegasus). En théorie, les clients de NSO ne peuvent faire usage du logiciel que pour lutter contre des réseaux terroristes ou criminels, mais l'enquête journalistique a démontré que ça n'a pas toujours été le cas. « Certains cas qui ont été révélés nous mettaient dans l'embarras et […] nous allons avoir une discussion poussée avec le client pour tenter de savoir la raison légitime pour laquelle il a utilisé notre système », a affirmé le responsable de la conformité chez NSO, Haim Gelfand, sur la chaîne i24 News. Sous le feu des critiques, Israël a annoncé ouvrir une enquête parlementaire afin de définir si le logiciel avait été utilisé à bon escient.

Et en Belgique ?
Chez nous, les coordonnées de Charles Michel se trouvent dans la liste. Ainsi que celles de son père. *Le Soir* et *Knack* ont aussi découvert que Carine Kanimba, fille de Paul Rusesabagina, a été espionnée par le Rwanda. Elle assure qu'elle va porter plainte et considère cette intrusion comme « un outil d'intimidations ». Mathieu Michel, secrétaire d'État à la digitalisation chargé notamment de la Protection de la vie privée, réagit : « Face à un logiciel qui sait entrer à ce point dans l'intimité des gens, le meilleur moyen de se défendre est de développer un logiciel qui nous protège. On doit développer une vraie capacité d'autonomie stratégique. Dans le plan de relance, entre 50 et 55 millions vont être consacrés à construire cette protection en matière de cyberdéfense. »