Tensions diplomatiques autour du logiciel espion Pegasus

RÉCIT - Du Maroc à la Hongrie, de l'Arabie saoudite à l'Inde, une vingtaine de pays sont accusés d'avoir espionné des communications privées de politiciens et journalistes grâce au logiciel Pegasus de la société israélienne NSO.

Par **Nicolas Barotte**
Publié il y a 1 minute,
Mis à jour il y a 1 minute

Selon des rapports publiés dimanche, l'entreprise NSO «Pegasus» (ici, les locaux à Herzliya près de Tel Aviv en 2016) a été liée à une liste de 50.000 numéros de smartphones. *JACK GUEZ/AFP*

La société NSO et son logiciel Pegasus étaient connus. Mais l'ampleur de l'espionnage qu'ils ont permis et ses dérives, y compris en France, vient d'être révélée grâce à une large enquête pilotée par Forbidden Stories, un consortium international de journalistes. Leader dans son domaine, l'entreprise israélienne a développé des capacités d'espionnage sans équivalent: une fois un téléphone infecté, il est possible d'intercepter toutes les données qui s'y trouvent et d'écouter toutes les conversations, même celles qui utilisent des messageries cryptées. Les messages sont captés au moment où ils sont lus par l'utilisateur. Plusieurs États auraient utilisé cette technologie contre leurs opposants et contre la presse.

Forbidden Stories a eu accès à une liste de 50.000 numéros de téléphones ciblés depuis 2016 par l'entreprise israélienne. Si le logiciel est censé être utilisé par des États pour la lutte contre le terrorisme international, Forbidden Stories et les 17 médias que l'organisation a réunis ont dénombré dans cette liste au moins 180 journalistes, 600 hommes et femmes politiques, 85 militants des droits humains ou encore 65 chefs d'entreprise. Un chef d'État et deux chefs de gouvernement européens figureraient aussi sur la liste. *«Nous ne parlons pas ici juste de quelques États voyous, mais d'une utilisation massive d'un logiciel espion par au moins une vingtaine de pays»,* a dénoncé la secrétaire générale d'Amnesty, Agnès Callamard.

«Ce sont des faits extrêmement choquants, et, s'ils sont avérés, extrêmement graves», a déclaré lundi le porte-parole du gouvernement, Gabriel Attal. *«Nous sommes extrêmement attachés à la liberté de la presse»*, a-t-il insisté. Si les accusations à l'encontre de NSO sont avérées, *«c'est complètement inacceptable»,* a dénoncé pour sa part la présidente de la Commission européenne, Ursula von der Leyen. Ce n'est pas la première fois que NSO est pointé du doigt. L'Arabie saoudite, notamment, a piraté en 2018 le téléphone du patron d'Amazon, Jeff Bezos.

En France, un millier de cibles a été dénombré

Une partie de ces cibles listées par Forbidden Stories, pas nécessairement toutes, ont pu être infectées par le logiciel Pegasus. L'Azerbaïdjan, le Rwanda ou le Maroc sont cités par le consortium. L'enquête a aussi révélé que des proches du journaliste saoudien Jamal Khashoggi, sauvagement assassiné par les services saoudiens, avaient été surveillés grâce au logiciel de NSO. En Hongrie, 300 cibles ont été identifiées. Mais le ministre hongrois des Affaires étrangères, Peter Szijjarto, a affirmé que les services de renseignement n'avaient pas eu recours à NSO.

En France, un millier de cibles a été dénombré. Des journalistes du *Monde*, de Mediapart, du *Canard enchaîné*, de l'AFP, de France Télévisions ou du *Figaro*, comme Éric Zemmour, figurent sur cette liste. Le Maroc serait à l'origine du ciblage pour une grande partie d'entre eux. Lundi après midi, Rabat a démenti les accusations.

> **Leur technologie est sans équivalent, mais beaucoup dans le domaine de la cybersécurité ne veulent plus être associés à eux**
>
> Lior Tabansky, chercheur à Tel-Aviv

Dès la publication de l'enquête, NSO avait elle aussi protesté. Fondée en 2009-2010, l'entreprise suscite des commentaires embarrassés en Israël. *«Ici, on dit de ceux qui travaillent pour NSO qu'ils vendent leur âme»*, explique Guillaume-David Deniel, un ancien collaborateur

de Kaymera, une des filiales de NSO. Kaymera développe des moyens de cyberprotection. *«Leur technologie est sans équivalent, mais beaucoup dans le domaine de la cybersécurité ne veulent plus être associés à eux»*, commente aussi Lior Tabansky, chercheur au Blavatnik Interdisciplinary Cyber Research Center à Tel-Aviv. *«Mais le marché est très lucratif»*, ajoute-t-il.

Récemment, après la multiplication des scandales, le groupe a commencé à vouloir polir son image. L'entreprise a ainsi embauché l'année dernière l'une des anciennes responsables de la communication de l'armée israélienne Ariella Ben Abraham. *«On parle des scandales, mais pas des enquêtes que NSO permet de dénouer»,* relativise Lior Tabansky, qui doute d'une surveillance généralisée grâce aux logiciels espions de l'entreprise. *«Cela coûte très cher, même pour une pétromonarchie très riche»,* dit-il.

La vente de produits de cybersurveillance de NSO est encadrée par le gouvernement israélien qui délivre les autorisations. Mais, en réalité, NSO a peu de limites. La seule contrainte est de ne pas proposer ses *«solutions»* à des adversaires d'Israël. En interne, l'entreprise est aussi censée disposer d'un système d'audit interne de ses clients. En juin, NSO a présenté sonpremier rapport annuel sur la transparence et la responsabilité. L'entreprise assure avoir *«déconnecté»* cinq de ses clients en raison d'abus et avoir interrompu sa collaboration avec cinq autres, en raison d'interrogations sur le respect des droits de l'homme. *S*urtout, NSO assure ne pas être responsable de l'usage de sa technologie, comme si elle avait anticipé le scandale.