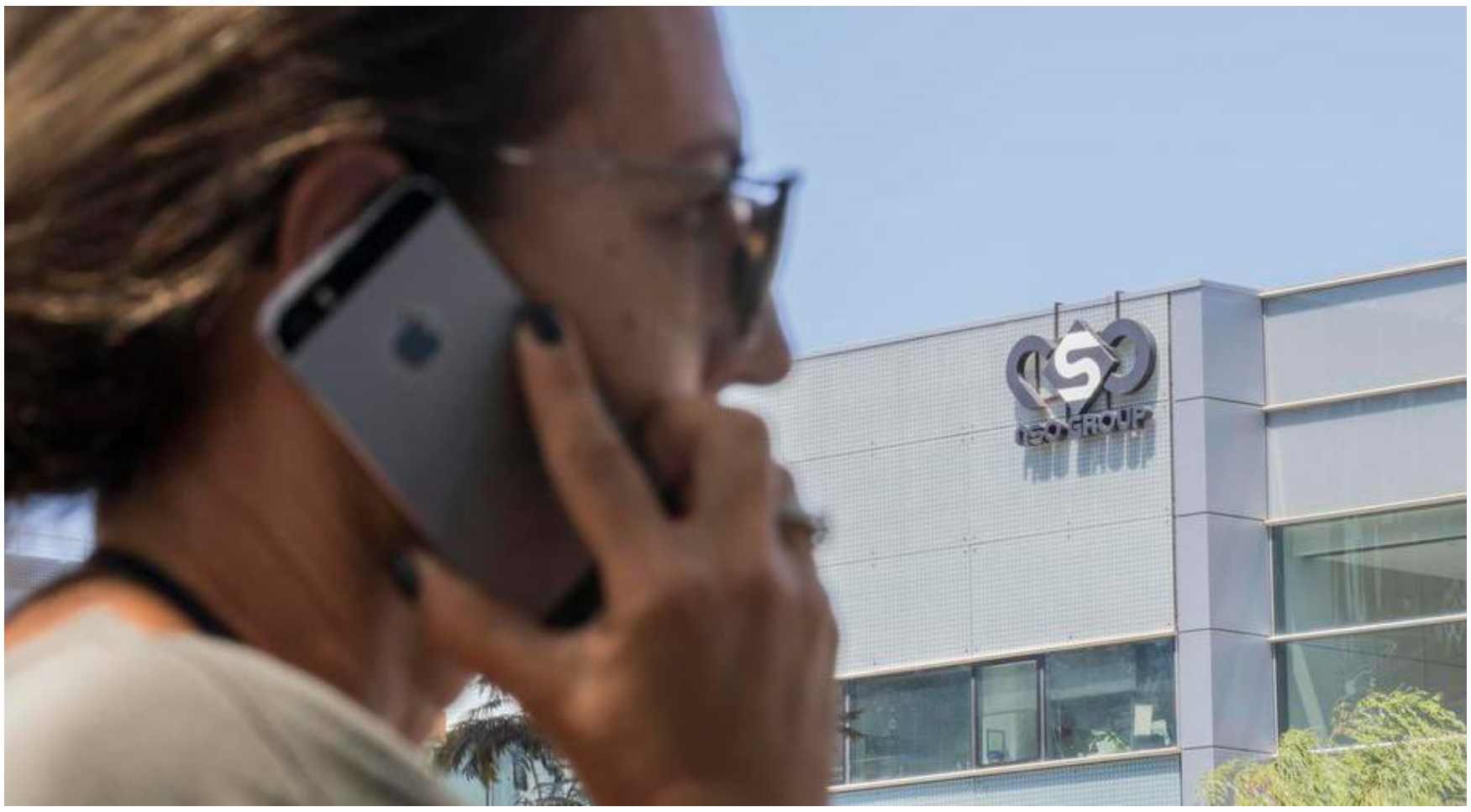

Le logiciel le plus connu de l'entreprise israélienne NSO, Pegasus, s'invite dans les smartphones, qu'ils fonctionnent sous iOS ou Android. Sans mot dire et – la plupart du temps – sans laisser de traces. © AFP.

lions de dollars comme l'a depuis révélé le média en ligne mexicain *Aristegui Noticias*. Un investissement que les autorités n'ont pas tardé à rentabiliser : plus de 15.000 numéros ont été sélectionnés par différents services mexicains au cours des seules années 2016 et 2017, ressort-il des données auxquelles « Forbidden Stories » et Amnesty, puis les médias partenaires, ont eu accès. Si cette surveillance est officiellement dédiée à la lutte contre les cartels, il apparaît que le cellulaire de Cecilio Pineda, le directeur de *La Voz de la Tierra Caliente*, assassiné le 2 mars 2017 par deux hommes à moto, avait été sélectionné quelques semaines avant le meurtre par un des clients mexicains de NSO. Une analyse approfondie de ce téléphone n'a cependant pu être menée, l'appareil ayant disparu après la mort du journaliste.

Carmen Aristegui, la fondatrice du média *Aristegui Noticias*, a elle aussi suscité l'intérêt de Pegasus. C'était en 2014 : « Au début, mon fils et moi avons commencé à recevoir des messages étranges sur nos téléphones portables », raconte-t-elle aux membres du « Pegasus Project ». « J'ai demandé à un ami qui m'a dit qu'il s'agissait sans doute d'un logiciel malveillant (…) Il m'a fallu un certain temps pour comprendre l'ampleur de l'attaque et du type de virus qui avait été introduit dans mon téléphone. J'étais d'abord résignée car au Mexique, nous avons toujours été espionnés. Lorsque j'ai appris qu'il s'agissait de quelque chose appelé Pegasus, ma réaction a été différente (…) Ces attaques sont inacceptables dans une démocratie. » En 2017, les experts canadiens du « Citizen Lab », avaient même établi qu'un scientifique et deux fonctionnaires mexicains favorables à une taxe sur les boissons gazeuses avaient été ciblés par des clients de NSO.

En Arabie saoudite, notre enquête révèle que des proches de Jamal Khashoggi, le chroniqueur du *Washington Post* assassiné le 2 octobre 2018 au consulat d'Arabie saoudite à Istanbul, ont également été sélectionnés après ce meurtre par un gouvernement client de NSO.

En Inde

En Inde, les numéros de trente journalistes ont été sélectionnés – ce qui ne signifie donc pas nécessairement qu'il y a eu tentative d'intrusion – par des clients de NSO ; ces journalistes travaillent notamment pour *The Hindu*, *Hindustan Times*, *The Indian Express*, *India Today* et *Tribune*, le site d'investigation Tehelka. Audité par Amnesty International, le téléphone portable de Paranjoy Guha Thakurta, un journaliste indépendant qui a notamment collaboré avec *India Today*, *NewsClick* et *Business India*, a ainsi rapporté plusieurs traces de contamination en 2018. « Pénétrer ainsi dans mon téléphone et chercher à savoir qui sont les personnes avec qui je parle a vraisemblablement pour objectif de savoir qui sont ceux qui nous fournissent des informations, à moi et mes collègues », s'inquiète Paranjoy Thakurta. « Nous parlons à un tas de gens sous couvert d'anonymat. Ils nous donnent des informations parce que leurs noms ne seront pas dévoilés. » Il a conscience que contrer l'espionnage numérique est de plus en plus compliqué, qu'il n'y a pas une façon de travailler qui soit « sûre à 100 % », « si ce n'est rencontrer votre interlocuteur en laissant votre téléphone au milieu d'un bar et en vous assurant que vous n'êtes pas survolé par un drone ».

Les téléphones de deux journalistes de *The Wire*, un média indien qui participe au « Pegasus Project », ont également été infectés.

Interrogé sur l'usage de Pegasus par nos confrères du *Washington Post*, le gouvernement indien a notamment répondu que « le ministre indien de l'électronique et des technologies de l'information a également déclaré en détail, y compris devant le Parlement, qu'il n'y avait pas eu d'interception non autorisée par les agences gouvernementales ». « Il est important de noter que les agences gouvernementales disposent d'un protocole d'interception bien établi, qui comprend l'approbation et la supervision de fonctionnaires de haut rang du gouvernement central et des gouvernements des Etats, pour des raisons claires et uniquement dans l'intérêt national. » Et que « les allégations sur la surveillance de certaines personnes par le gouvernement ne repose sur aucune base concrète, sur aucune vérité ».

En Hongrie

Au pays de Viktor Orban, plusieurs personnalités ont été aussi visées par le logiciel espion. Notamment Szabolc Panyi, un journaliste de *Direckt36* qui a découvert lors du « Pegasus Project », auquel il participe, que son mobile avait été ciblé par Pegasus : « Voir mon nom en compagnie de politiciens et de criminels qui apparaissent aux informations et dans des rapports de police, c'était choquant », explique-t-il. « Il y a dans ce pays des gens qui considèrent qu'un journaliste est aussi dangereux qu'une personne soupçonnée de terrorisme. »

En juin 2018, deux mois après la réélection de Viktor Orban, c'est Zoltan Varga, qui contrôle « Central Media Group », qui apparaît dans une liste de cibles potentielles. Le téléphone d'Arien Beauduin, un Belgo-Canadien, a lui aussi été visé après qu'il a participé à une manifestation contre le régime, en 2018 mais rien n'indique, selon le Security Lab d'Amnesty qui a analysé le téléphone de M. Beauduin, qu'il y a eu intrusion. « Les écoutes téléphoniques ne sont possibles et autorisées que si elles se font conformément à la loi », commente à nos confrères du *Monde* la ministre hongroise de la Justice, Judit Varga. « Elles doivent donc avoir une justification, comme dans chaque pays. »

Interrogé par le *Süddeutsche Zeitung* dans le cadre de ce projet, le gouvernement hongrois fait savoir que « la Hongrie est un Etat démocratique régi par des textes de loi et que par conséquent, lorsqu'il s'agit d'individus, il (l'Etat hongrois) a toujours agi et continue d'agir conformément à la loi en vigueur. »

Réaction de NSO

Le groupe NSO rappelle qu'il ne déploie pas lui-même Pegasus, il ne fait que fournir des licences aux gouvernements et aux autorités. Néanmoins, précise l'entreprise, si des plaintes crédibles relatives à une mauvaise utilisation nous parviennent, nous continuerons à enquêter et en fonction des résultats de ces investigations, nous prendrons les mesures appropriées. Ce qui peut signifier empêcher un client d'encore utiliser le système, ce que NSO a la volonté et la capacité de faire en cas d'abus. » Enfin, l'entreprise israélienne soutient que sa technologie a aidé à prévenir des attaques terroristes, des fusillades, des attentats suicides… Bref, « la mission de NSO est de sauver des vies, une mission que l'entreprise mène indéfectiblement, malgré les incessantes tentatives de la discréditer sur base de fausses allégations ».

5

Recoupements et analyses

Le fait qu'un numéro figure sur la liste ne signifie pas qu'il a été l'objet d'une attaque, la fuite de ces données est seulement le point de départ de l'enquête. Cette dernière, qui a duré plusieurs mois, a été mise à profit pour identifier un maximum de ces numéros de portables, récolter des documents afin de contextualiser les pratiques de NSO et surtout de certains de ses clients, mener des entretiens avec des personnes dont les coordonnées téléphoniques figuraient dans la liste, en convaincre certaines de soumettre leur appareil à une analyse technique, menée par le Security Lab d'Amnesty et doublée d'un second audit, réalisé par le Citizen Lab de Toronto. Car si le logiciel espion Pegasus a pour redoutable caractéristique d'effacer les traces de son passage, certaines empreintes subsistent néanmoins dans les relevés d'utilisation (les « logs ») des téléphones qui ont été visés par le logiciel. Ces analyses sont beaucoup plus efficaces sur iPhone que sur Android, notamment parce que le système d'exploitation de Google ne permet d'accéder qu'à peu de fichiers techniques sur le fonctionnement du système. Les laboratoires ont pu confirmer une infection ou tentative d'infection avec Pegasus dans 85 % des cas, soit 37 au total. Ce taux remarquablement élevé étant donné que le logiciel espion est censé être indétectable. JO.MA.

6

Puis-je me protéger ?

Pegasus requiert, pour être vendu, une licence d'exportation du ministère israélien de la Défense. Il tient bien plus de l'arme numérique que d'un gadget développé par quelques geeks. Autant dire qu'il est très difficile, sinon impossible, de s'en prémunir. « Les vecteurs d'attaque ont changé au cours du temps », explique Claudio Guarnieri. Les clients de NSO ont abandonné l'envoi de SMS dans lesquels ont été intégrés des liens malveillants, ils se reposent aujourd'hui sur des failles de sécurité que personne ou pratiquement personne n'a encore documentées. Leurs attaques sont indétectables. « Pour les cibles, il est de plus en plus difficile de se douter de quoi que ce soit, il n'y a aucun signe qui leur ferait comprendre que quelque chose est en train de se passer. » Il est néanmoins plus que recommandé de mettre à jour son téléphone aussi souvent que recommandé afin de bénéficier des derniers correctifs publiés par les développeurs de logiciels. Une connexion VPN contrarie également certaines tentatives d'intrusion. JO.MA.

7

La Belgique est-elle cliente de NSO ?

Selon deux sources, qui souhaitent conserver l'anonymat et qu'ont interrogées nos collègues de *Die Zeit*, la Belgique figurerait parmi les clients de NSO. Des propos réitérés par une troisième source, cette fois auprès de notre collègue de *Knack*. Ni la Sécurité d'Etat, ni le Service de renseignement militaire (SGRS), ni la police fédérale n'ont toutefois voulu commenter, évoquant une information « confidentielle ». Bref, nous ne pouvons affirmer aujourd'hui que la Belgique est cliente de NSO. Mais quel que soit le logiciel qu'utilisent les services de sécurité belge, son déploiement ne peut se faire que sous le contrôle d'un juge d'instruction lorsqu'il s'agit d'un dossier judiciaire, sous celui de la commission Bim (spécifiquement chargée du contrôle des méthodes spécifiques et exceptionnelles de recueil des données) lorsque la demande émane d'un de deux services de renseignement. En matière de renseignement encore, un contrôle a posteriori est exercé par le Comité R. JO.MA.

8

Que répond NSO ?

Dans une lettre envoyée à Forbidden Stories et ses partenaires, l'entreprise NSO a affirmé que l'enquête du consortium était basée sur de « mauvaises suppositions » et des « théories non corroborées ». L'entreprise israélienne a insisté sur le fait que le travail des journalistes du Projet Pegasus reposait sur une « interprétation erronée des données fuitées provenant d'informations librement accessibles et basiques telles que les services de recherche HLR, qui n'ont aucun rapport avec la liste des clients cibles de Pegasus ou tout autre produit de NSO ». HRL (Home Location Register) est une base de données essentielle au fonctionnement des réseaux téléphoniques. Une personne ayant une connaissance directe du fonctionnement de NSO, qui a accepté de parler anonymement, a confié aux membres du Projet Pegasus que « les services de recherche HRL sont une étape clef pour déterminer les caractéristiques d'un téléphone, notamment s'il est allumé ». L'entreprise NSO a aussi déclaré qu' « elle continuerait à enquêter sur toutes les allégations crédibles d'utilisation abusive de son logiciel ». JO.MA.