L’UE et la pandémie vont-elles ouvrir la voie à une surveillance mondiale israélienne ?

Par Ali Abunimah, 13 avril 2020

Le ministre israélien de la Défense Naftali Bennett, à gauche, avec l’ambassadeur Emanuele Giaufret, espère maintenant que d’autres pays achèteront un système de repérage du coronavirus fabriqué par une entreprise d’espionnage impliquée dans l’assassinat du journaliste saoudien Jamal Khashoggi. (via Twitter)

La pandémie du coronavirus est une opportunité considérable pour les gouvernements et les entreprises d'espionnage d'étendre leur portée, y compris dans la vie privée des individus.

Les autorités de santé publique affirment qu'un tracking efficace sera essentiel pour mettre fin à de longs confinements et mettre rapidement un stop à de nouveaux rebonds du virus, au moins jusqu'à ce qu'un vaccin soit développé.

Cela signifie que les technologies de surveillance qui promettent d'identifier rapidement quiconque est exposé au virus peuvent certainement trouver un marché mondial. Le danger étant que ce genre de surveillance intrusive devienne permanent.

Le célèbre NSO Group est l'une des entreprises qui cherche à tirer parti de cette opportunité.

C'est la société qui produit le logiciel malveillant appelé Pegasus qui peut discrètement s'insérer dans le téléphone portable d'une cible.

Il peut ensuite être utilisé pour renvoyer presque toutes les informations privées à ceux qui espionnent, y compris les enregistrements, les captures d'écran, les mots de passe, mails et textes.

L'industrie technologique tant vantée d'Israël a des liens profond avec l'appareil militaire et d'espionnage du pays, qui

utilise les Palestiniens sous occupation armée comme d'involontaires cobayes pour des systèmes qui sont maintenant mis en vente pour d'autres pays.

Et on découvre maintenant que les gouvernements européens sont prêts à profiter de cette structure abusive et oppressive, au prétexte de combattre la pandémie.

Pegasus du Groupe NSO, qui n'est vendu qu'à des gouvernements, a été abusivement utilisé contre des journalistes et des militants des droits de l'Homme dans des dizaines de pays. Parmi les utilisateurs suspectés, il y a le Maroc, le Mexique, les Emirats Arabes Unis, le Bahreïn et le Kazakhstan.

Pegasus a également été impliqué dans l'assassinat de Jamal Kashoggi, le journaliste saoudien attiré dans le consulat de son pays en 2018 à Istanbul et sauvagement assassiné et dépecé.

Amnesty International, dont l'équipe a été ciblée grâce au logiciel malveillant du Groupe NSO, poursuit la société en justice pour faire stopper son rôle dans la surveillance abusive.

Facebook intente également un procès à NSO Group pour avoir compromis sa plate-forme de messagerie WhatsApp afin d'aider des gouvernements à espionner environ 1.400 personnes.

« Tentative cynique »

Aujourd'hui, les experts de la vie privée et pour les droits humains s'inquiètent du fait que NSO Group soit à la pointe d'un effort de surveillance du coronavirus sponsorisé par le gouvernement israélien qui pourrait être adopté dans d'autres pays.

Le ministre israélien de la Défense Naftali Bennett s'est vanté le mois dernier que son ministère et l'armée israélienne aient travaillé avec NSO Group au développement d'un système qui permette de donner aux Israéliens une évaluation de la probabilité qu'ils avaient d'être infectés par le nouveau coronavirus.

D'après le journal financier israélien Globes, « *ce système collectera des informations sur les Israéliens, les mettra à jour en temps réel et attribuera à chaque Israélien un 'taux d'infection' sur une échelle de un à 10* ».

Vice.com a fait des recherches sur la technologie de NSO Group.

Le site décrit le système fabriqué par NSO Group, et un système semblable développé par l'entreprise italienne Cy4Gate, comme « *essentiellement des outils de surveillance de masse qui aideraient les gouvernements et les autorités de santé à garder la trace des mouvements de chaque citoyen et à rester en contact avec eux* ».

Dans ce but, selon Vice.com, NSO Group a « *adapté l'interface utilisateur et l'outil analytique qu'il avait déjà développés pour pouvoir l'utiliser parallèlement à son puissant logiciel malveillant connu sous le nom de Pegasus, qui peut pirater les téléphones portables et en extraire des données comme les photos, les messages et les appels téléphoniques* ».

Ce nouveau système, appelé Fleming, « *permet aux analystes de dépister où vont les gens, qui ils rencontrent, combien de temps, et où* ».

Les individus sont censés se voir attribuer un numéro d'identification secret pour protéger leur vie privée, mais une source de NSO Group a affirmé à Vice.com que le gouvernement peut enlever l'anonymat « *lorsque nécessaire* ».

En réalité, c'est du piratage en temps réel.

« *Il s'agit d'une tentative extrêmement cynique de la part d'une célèbre entreprise de logiciels espions pour se lancer dans la surveillance de masse* », a affirmé John Scott-Railton, chercheur à Citizen Lab de l'université de Toronto, à Vice.

Citizen Lab a joué un rôle juridique essentiel en dévoilant comment le logiciel malveillant de NSO Group a été détourné de son usage à travers le monde.

« *Chaque citoyen dans le monde veut revenir à la normale dès que possible. La ruée vers l'or de la technologie de surveillance pourrait facilement signifier qu'il y a une attente normale de vie privée à laquelle il nous sera très*

difficile de revenir », a ajouté Scott-Railton.

Comme le fait remarquer Vice, les détenteurs de mobiles dans des pays comme l'Italie, l'Allemagne, l'Autriche, l'Espagne, la France, la Belgique et le Royaume Uni « *partagent déjà l'emplacement de leurs courses avec leurs gouvernements respectifs dans un effort pour dépister l'expansion du virus* ».

Enthousiasme européen

Alors qu'il n'y a aucun rapport fait par ces gouvernements qui utilisent les systèmes du NSO Group, il existe des signes troublants selon lesquels l'Union Européenne et ses membres cherchent à adopter la technologie de surveillance de masse sous couvert de lutte contre le COVID-19.

Lundi, l'ambassade des Pays Bas à Tel Aviv a déclaré dans un tweet qu'elle « cherchait des sociétés hollandaises qui voudraient s'associer à un partenaire israélien afin de soumissionner pour une offre unique de solutions numériques intelligentes au Corona par le ministère de la Santé des Pays Bas.

https://twitter.com/NLinIsrael/status/1249591569155571716?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1249591571638636544&ref_url=https%3A%2F%2Felectronicintifada.net%2Fblogs%2Fali-abunimah%2Fwill-eu-and-pandemic-pave-way-israeli-global-surveillance

Et Emanuele Giaufret, ambassadeur de l'Union Européenne à Tel Aviv, a publié un courrier dans The Jerusalem Post où il se

vante de la façon dont le bloc des 27 membres « *exploite sa recherche scientifique et technologique pour lutter contre le COVID-19* », un effort qui comporte « *des projets de coopération avec Israël* ».

https://twitter.com/EUinIsrael/status/1249628363792187393

D'après Giaufret, l'UE a affecté environ 150 millions de dollars de son programme scientifique Horizon 2020 « *au financement d'équipes scientifiques à travers l'Europe ainsi que dans des pays partenaires, dont Israël, pour aider à trouver rapidement un vaccin contre le COVID-19* ».

Il ajoute que le but de cet effort, « *c'est d'améliorer les diagnostics, les préparatifs, la gestion clinique et les traitements* ».

Ces activités sont suffisamment vastes pour y inclure les efforts de financement de la surveillance, surtout quand Horizon 2020 a déjà servi ces dernières années à financer Elbit Systems, entre autres sociétés de l'industrie guerrière d'Israël.

Elbit, qui fait actuellement sa promotion en tant que fournisseur de technologie pour combattre la pandémie.

Bennett, le ministre israélien de la Défense, a clairement affirmé qu'il voulait exporter le système de surveillance du coronavirus de NSO Group.

Et Sky News a rapporté au début du mois que NSO Group a « *contacté quantité de pays occidentaux pour leur envoyer son logiciel de dépistage du coronavirus* ».

Testé sur les Palestiniens

La maltraitance israélienne sur les Palestiniens, y compris sur ses propres citoyens, pendant la pandémie a poursuivi le même schéma de racisme, de violence et de négligence qui sont fondateurs de cet Etat.

Les travailleurs palestiniens de Cisjordanie occupée ont peu d'autre choix que de travailler pour des employeurs israéliens s'ils veulent nourrir leurs familles.

Quand ils sont en Israël, ils sont exposés au virus qu'ils risquent alors de rapporter dans leurs propres communautés.

Mais l'indifférence systématique d'Israël pour la santé et la sécurité des Palestiniens ne l'a pas empêché de les obliger à être des sujets d'expérience pour ses technologies de contrôle et de surveillance.

« *Les Palestiniens qui cherchent à vérifier si leurs permis de séjour en Israël sont encore valides ont reçu l'instruction par Israël de charger une application qui permet à l'armée d'accéder à leurs téléphones portables* », a rapporté la semaine dernière le journal de Tel Aviv Haaretz.

« *L'application permettrait à l'armée de pister la localisation du portable des Palestiniens, ainsi que d'accéder aux avis qu'ils reçoivent, aux fichiers qu'il chargent et sauvegardent, et à la caméra de l'appareil*. »

Haaretz n'explique pas comment un accès aussi indiscret a quoi que ce soit à voir avec le combat contre le virus, et il ne dit pas non plus qui a fabriqué cette application particulière.

Mais les médias israéliens ont confirmé que la branche de guerre informatique de l'armée israélienne, Unité 8200, est impliquée dans le projet de dépistage du coronavirus de NSO Group.

En 2014, des vétérans de l'Unité 8200 ont révélé que « *la population palestinienne sous régime militaire est entièrement exposée à l'espionnage et à la surveillance du renseignement israélien* ».

Les agents israéliens ont avoué que les informations qu'ils ont aidé à collecter et à stocker « *nuisent à des gens innocents* ».

« *On s'en sert pour des persécutions politiques et pour créer des divisions à l'intérieur de la société palestinienne en recrutant des collaborateurs et en montant des parties de la société palestinienne contre elle même* », ont-il ajouté.

Maintenant, le reste du monde peut obtenir le traitement des Palestiniens.

« *Ce qui se passe en Palestine ne reste pas en Palestine* », note le groupe de recherche Who Profits sur un nouveau site internet consacré à la surveillance de la façon dont la crise du COVID-19 se développe dans le contexte de l'occupation israélienne.

« *Une raison essentielle pour laquelle Israël cherche perpétuellement à diversifier son arsenal de répression est qu'il peut ensuite le transformer en profit économique et en gains politiques*. »

La pandémie du coronavirus est l'opportunité parfaite pour Israël de mettre son espionnage sur le marché de cette façon.

Et tout indique que l'Union Européenne – en conformité avec son record sans faille de complicité – est prête à aider Israël à répandre sa surveillance partout dans le monde.

Traduction : J. Ch. pour l'Agence Média Palestine

Source : The Electronic Intifada

A lire également sur ce sujet, ce communiqué d'Amnesty International en date de Septembre 2019:

L'entreprise israélienne de

logiciels espions NSO doit donner suite à ses engagements