Predator Files

CYBERSURVEILLANCE

Jusque mardi, « Le Soir » publie plusieurs épisodes des « Predator Files », enquête collaborative coordonnée par le réseau EIC (European Investigative Collaborations). Sur base de documents confidentiels, celle-ci dévoile les coulisses de l'alliance Intellexa, qui depuis l'Europe a commercialisé le logiciel espion Predator.

Predator Files : l'Europe toujours inc de contrôler la vente de logiciels espi

© MEDIAPART/SIMON TOUPET.

Depuis septembre 2021, un règlement européen encadre plus strictement les exportations d'outils de cybersurveillance. Ce texte, dont certaines ambitions initiales ont été revues à la baisse à cause de la réticence de certains Etats, peine à convaincre de son efficacité.

ARTHUR SENTE (AVEC L'EIC ET FRAGDENSTAAT)

Le 15 novembre 2021, le ministère grec des Affaires étrangères accordait deux licences d'exportation à la société Intellexa S.A., établie à Athènes. La première concernant un produit « conçu pour l'extraction de données à partir d'appareils mobiles et la gestion de la collecte de données ». La seconde relative à « un système de traçage et d'interception wifi conçu pour extraire et analyser les données d'appareils mobiles connectés à un wifi ».

Un cocktail de technologie espionne dont le destinataire final officiellement mentionné dans le document n'est autre que l'Agence nationale antifraude de Madagascar. Un Etat traînant derrière lui un bilan contesté en matière de respect des droits humains.

Dans sa demande, la société fondée par le vétéran de l'armée israélienne Tal Dilian (au cœur de l'enquête Predator Files) tient cependant à rassurer les autorités grecques : ses produits serviront, d'après leur acheteur final, « à assurer la sécurité en prévenant les activités criminelles et terroristes ».

L'appellation commerciale du système espion destiné à être exporté n'est pas mentionnée dans la requête soumise aux autorités grecques. Tout converge cependant pour indiquer qu'il s'agit du logiciel espion Predator. Lequel sera effectivement délivré à Madagascar, comme en attestent des documents obtenus dans le cadre de l'enquête Predator Files à laquelle quinze médias, dont *Le Soir*, ont participé sous la coordination du réseau European Investigative Collaborations (EIC).

L'épisode en témoigne : la technologie d'espionnage *made in Europe* s'exporte encore hors des frontières de l'Union, notamment à destination des Etats dont l'engagement dans le respect des droits humains peut à tout le moins être mis en cause.

« Un problème européen »

La Commission d'enquête Pega, mise sur pied en 2022 dans la foulée du scandale Pegasus (du nom d'un logiciel espion israélien utilisé à l'encontre de milliers de cibles, notamment en Europe) et des révélations du consortium Forbidden Stories (dont *Le Soir* fait partie) à ce sujet, ne dit d'ailleurs rien d'autre.

Son rapport, publié en mai 2023 et approuvé par le Parlement européen, estime qu'encore aujourd'hui « l'Europe est un hub pour l'exportation de *spywares* vers des dictatures et des régimes oppressifs ». L'eurodéputée néerlandaise Sophie In't Veldt (groupe Renew), qui a joué le rôle de rapporteuse dans cette Commission, va encore plus loin en parlant de l'émergence de « vrais hotspots ». « Les Pays-Bas, la France, l'Irlande, le Luxembourg, Chypre, la Bulgarie et beaucoup d'autres pays sont activement en train d'œuvrer à l'espionnage de personnes de par le monde », dit-elle. « C'est un problème européen. »

Et cela en dépit de la refonte récente du règlement de l'Union relatif à l'exportation de biens à double usage (une appellation catégorisant tout type de bien sensible pouvant servir à la fois à des fins militaires et civiles), entré en vigueur le 9 septembre 2021.

La refonte était devenue pressante au cours de la décennie passée, à la suite de multiples scandales exposant des entreprises basées dans l'Union et pincées pour avoir armé certains régimes très durs dans la foulée des Printemps arabes.

En France, la société Nexa (figure centrale des Predator Files, autrefois connue sous le nom d'Amesys, voir nos éditions du 6 octobre) a notamment vendu son système de surveillance massive du réseau internet à la Libye, puis à l'Egypte, sans que le SBDU, l'autorité française chargée de contrôler son exportation, n'y trouve à redire.

Autre exemple ayant fait grand bruit : l'octroi en 2015 d'une licence globale par les autorités italiennes à la société Hacking Team, suivi de son retrait en 2016 à l'aune d'une fuite exposant son business dans des pays tels que le Soudan, l'Arabie saoudite et l'Egypte.

Résultat : la Commission a fini par mettre sur la table fin 2016 une proposition pour recalibrer son régime d'exportation, datant alors de 2009. Avec la promesse d'intégrer dans son règlement la question spécifique d'un meilleur contrôle des flux sortants d'outils de cybersurveillance. Il aura fallu cinq années pour voir ce chantier aboutir.

Actuellement les Etats membres demeurent compétents en matière d'octroi de licences d'exportation de biens à double usage, tout en devant se plier à certaines obligations fixées dans la réglementation européenne, mais aussi dans un accord multilatéral liant à l'heure actuelle 42 pays (dont les Etats-Unis, la Russie et tous les Etats membres sauf Chypre) : l'arrangement de Wassenaar.

Ce régime, créé en 1995, repose sur une règle simple. Tout type de bien repris dans une fameuse liste de produits sensibles sur laquelle ses membres se sont mis d'accord, doit faire l'objet d'une autorisation à l'exportation. Et cette liste a été calquée telle quelle dans la réglementation européenne.

Ce n'est cependant qu'à partir de 2012 que des catégories englobant certains outils de cybersurveillance ont été intégrées à la liste de Wassenaar – et dans la foulée à sa transposition européenne. Les composants et programmes destinés à la production de « logiciels intrusifs », par exemple, y sont maintenant inclus, bien que la définition donnée à ce terme soit sujette à débat car elle comporterait des angles morts. Les systèmes de surveillance de communications sur le réseau internet sont également repris dans la liste.

Mais ces catégories sont limitées, étroites et figées. Pendant que l'industrie de la cybersurveillance avance à pas de géant, tout en innovant sans cesse. Et ce n'est pas la seule critique à l'égard de Wassenaar, qui « prévoit une obligation d'information mais pas de disposition de contrôle ou de mesure contraignante », synthétise Katia Roux, chargée de plaidoyer chez Amnesty international. « Très clairement, l'arrangement de Wassenaar n'empêche pas les abus. »

Au nom de la compétitivité

Pour mieux suivre l'évolution technologique, rendre son régime de contrôle plus durable et s'affranchir de l'inertie propre à Wassenaar, la Commission a voulu en 2016 consacrer dans sa proposition de règlement la création d'une liste spécifiquement européenne d'outils de cybersurveillance soumis d'office à un contrôle à l'exportation. Selon ce plan initial, cette liste « autonome » aurait pu être complétée au fil du temps sur la base de procédures définies.