Logiciel Pegasus : fedpol doit communiquer sur l'(in)existence d'un contrat avec NSO Group

Livio di Tria et Kastriot Lubishtani, le 28 février 2022

Le PFPDT recommande à l'Office fédéral de la police (fedpol) de communiquer sur l'existence ou l'inexistence d'un contrat conclu avec NSO Group qui commercialise le logiciel espion Pegasus.

Recommandation PFPDT du 25 janvier 2022, Fanti c. Office fédéral de la police (fedpol)

I. En fait

Au mois de juillet 2021, une enquête journalistique internationale baptisée « Projet Pegasus » révèle que le logiciel espion israélien Pegasus a été utilisé par onze États pour espionner des journalistes, opposants politiques, militants des droits de l'homme et chefs d'États. Le 11 août qui suit, la RTS publie un article révélant que les autorités suisses utilisent un logiciel espion israélien pour résoudre certaines enquêtes. L'Office fédéral de la police (fedpol) ne précise pas toutefois s'il s'agit du logiciel Pegasus.

Quatre jours après la publication de l'article de la RTS, Sébastien Fanti adresse en sa qualité de citoyen une demande d'accès fondée sur la LTrans à fedpol afin d'obtenir le contrat conclu avec la société israélienne NSO Group pour l'utilisation de tout logiciel développé par cette firme.

Le 22 septembre 2021, fedpol refuse la demande en alléguant (i) une entrave à l'exécution de mesures concrètes prises par fedpol conformément à ses objectifs (art. 7 al. 1 let. b LTrans), ainsi que le risque de compromettre (ii) la sûreté intérieure ou extérieure de la Suisse (art. 7 al. 1 let. c LTrans) et (iii) les relations entre la Confédération et les cantons ou les relations entre cantons (art. 7 al. 1 let. e LTrans). En particulier, fedpol refuse d'informer le requérant quant à l'existence ou l'inexistence d'un tel contrat.

Une demande de médiation est déposée par le requérant le 12 octobre 2021 auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT). Invité à se déterminer par écrit, fedpol a persisté dans ses conclusions et encore allégué que la LTrans ne serait pas applicable en raison de l'exception prévue par l'art. 67 de la Loi sur le renseignement

(LRens). La médiation n'ayant pas abouti, le PFPDT rend la présente recommandation.

II. En droit

Dans un premier temps, le PFPDT analyse si l'art. 67 LRens exclut du champ d'application de la LTrans les documents requis. Cette disposition prévoit que la LTrans ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations. Cette exception ne doit pas être comprise comme excluant intégralement les documents détenus par le Service du Renseignement de la Confédération (SRC) du champ d'application de la LTrans. Seuls les documents précités le sont, qu'ils soient détenus par le SRC ou par une autre entité de l'administration fédérale, indépendamment de la question de savoir si cette autorité avait le droit de détenir de tels documents.

En l'espèce, le PFPDT est d'avis que la LRens, conformément à son art. 1, n'a pas vocation à s'appliquer à fedpol, mais uniquement aux activités du SRC. De plus, et en l'absence de toute argumentation, le PFPDT ne voit pas dans quelle mesure l'exception de l'art. 67 LRens pourrait être soulevée par fedpol.

Dans un deuxième temps, le PFPDT analyse dans quelle mesure les intérêts soulevés par fedpol pour refuser l'accès aux documents souhaités sont admissibles. Faute d'une réelle motivation par fedpol, il écarte tout d'abord l'art. 7 al. 1 let. e LTrans de manière expéditive.

En ce qui concerne le risque d'entrave à l'exécution de mesures concrètes prises par fedpol (art. 7 al. 1 let. b LTrans), le PFPDT rappelle que cette exception doit être interprétée de manière restrictive et uniquement si la mesure concrète prise par l'autorité est sérieusement compromise par la divulgation du document. Autrement dit, le secret de la mesure doit représenter la clé de son succès (p. ex. la divulgation du document révélerait une mesure de surveillance en cours) et doit être démontrée avec sérieux par l'autorité saisie. Faute d'une telle interprétation, l'exception permettrait de justifier un refus d'accès à un grand nombre de documents.

Dans le cas présent, fedpol se contente d'une argumentation générale sans démontrer quelle mesure risquerait d'être sérieusement compromise ni en quoi le secret représenterait la clé de son succès. À cela s'ajoute encore le fait que fedpol a déjà communiqué ouvertement sur le recours à des programmes informatiques dans le cadre de la poursuite pénale, sans que cela n'entrave les mesures de surveillance en question. Pour ces raisons, le PFPDT écarte cette exception.

Le risque que la sûreté intérieure ou extérieure de la Suisse soit compromise (art. 7 al. 1 let. c LTrans) vise essentiellement à maintenir les activités policières, douanières, de renseignement et militaires. L'exception doit ainsi permettre de maintenir secrètes les mesures destinées à préserver l'activité du gouvernement en cas de situation extraordinaire, d'assurer l'approvisionnement économique ainsi que les informations sur des détails techniques ou sur l'entretien de matériel d'armement, ou de celer les informations qui conduiraient à entraver la sécurité d'infrastructures importantes (FF 2003 1807, 1851).

En l'espèce, il apparaît que le public est déjà informé de l'acquisition de programmes permettant de surveiller la correspondance et de leur existence, que ce soit par l'intermédiaire de débats parlementaires ou de documents officiels déjà publiés. Le PFPDT mentionne ici le Rapport explicatif de la révision de l'Ordonnance sur les émoluments pour les décisions et les prestations de fedpol dont une partie relève l'acquisition de programmes informatiques spéciaux permettant aux autorités de poursuite pénale de mettre en œuvre des mesures de surveillance. Le PFPDT est donc d'avis que la divulgation du contrat, ou à tout le moins de son existence, n'est pas en mesure de compromettre la sécurité intérieure ou extérieure de la Suisse, une telle information étant déjà courante pour d'autres logiciels.

Au vu de ce qui précède, le PFPDT recommande à fedpol de renseigner le requérant sur l'existence ou l'inexistence d'un éventuel contrat conclu avec la firme NSO Group et, cas échéant, de lui accorder l'accès à celui-ci.

III. Commentaire

Selon nos informations, fedpol a décidé de ne pas suivre la recommandation du PFPDT et a maintenu sa position initiale dans une nouvelle décision contre laquelle le requérant entend former recours au Tribunal administratif fédéral.

Sur le fond, le résultat auquel parvient le PFPDT doit être approuvé, d'autant plus que la présente recommandation s'inscrit dans un contexte politique particulièrement tendu au vu des récentes divulgations explosives par la presse internationale, en particulier en ce qui concerne le nombre de cibles au sein de la société civile (avocats, journalistes, militants des droits de l'homme) qui ont été infectées par le logiciel israélien Pegasus. S'il est légitime pour un État de procéder à des mesures de surveillance, celles-ci n'en sont pas moins soumises à des restrictions et des cautèles précises au vu de la gravité de l'atteinte qu'elles peuvent emporter en particulier au droit au respect de la vie privée, mais aussi à la liberté d'information lorsqu'elles visent des journalistes (voir notamment arrêt Grande Chambre CourEDH du 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni). Compte tenu des révélations de

la presse, il y a un besoin accru d'information selon nous.

Bien qu'il n'existe aucune jurisprudence spécifique quant à Pegasus à ce jour, le Contrôleur européen de la protection des données s'est toutefois positionné le 15 février 2022 sur l'utilisation de ce logiciel. Selon celui-ci, la mesure la plus efficace afin de protéger les droits fondamentaux des résidents de l'Union européenne serait d'interdire le développement et le déploiement de tels outils de surveillance. Conscient que des États seraient malgré tout susceptibles d'acquérir de tels outils faute d'une interdiction légale, le Contrôleur établit une liste de huit étapes à respecter pour assurer le respect des droits fondamentaux des résidents de l'Union européenne.

Le raisonnement du PFPDT quant à l'application de l'art. 67 LRens à fedpol est néanmoins discutable. Il a en effet souligné que « fedpol n'avait pas indiqué dans son argumentaire de quelle manière cette disposition spéciale réglant l'activité du SRC (art. 1 LRens) lui était également applicable ». Or il nous semble qu'est uniquement décisive la nature du document en cause (« documents officiels portant sur la recherche d'informations »), indépendamment de l'autorité qui le détient, même s'il est à l'origine créé et détenu par le SRC en application de ses tâches légales. Ainsi, l'art. 67 LRens pourrait bel et bien trouver à s'appliquer à d'autres autorités que le SRC qui détiendraient un document visé par cette disposition.

Il est en outre intéressant de souligner le PFPDT n'a pas le droit de dévoiler dans le cadre de la procédure des informations qui pourraient porter atteinte à un des intérêts protégés par les dispositions de la LTrans (art. 13 al. 2 OTrans). Pour cette raison, il ne donne aucun renseignement quant à l'(in)existence d'un hypothétique contrat entre la Confédération et NSO Group.

Pour terminer, il y a lieu de mentionner que le Conseil fédéral a décidé le 16 février 2022 d'ouvrir une procédure de consultation relative à la révision des ordonnances de mise en œuvre de la Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication. Une consultation dure actuellement jusqu'au 23 mai 2022. La révision des ordonnances sur la surveillance des télécommunications est justifiée par le fait que la technologie 5G exige de nouveaux types de renseignements et de surveillances pour que la surveillance puisse être maintenue.

Proposition de citation : Livio di Tria / Kastriot Lubishtani, Logiciel Pegasus : fedpol doit

communiquer sur l'(in)existence d'un contrat avec NSO Group, 28 février 2022 *in* www.swissprivacy.law/129

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.