_swissprivacy.law

Les mesures de surveillance secrètes à l'aune de la LTrans

Mallorie Ashton-Lomax, le 18 décembre 2025

Le Tribunal fédéral confirme que la sécurité intérieure et extérieure de la Suisse constitue une exception à la divulgation du logiciel (GovWare) utilisé par les autorités de poursuite pénale suisses dans le cadre des mesures de surveillance secrètes prévues par le CPP.

Arrêt du Tribunal fédéral 1C_105/2024 du 1er septembre 2025

En fait

À la suite d'un reportage de la RTS dévoilant l'utilisation du logiciel Pegasus par plusieurs Etats, un avocat dépose auprès de l'Office fédéral de la police (Fedpol) une demande fondée sur la LTrans dans le but d'obtenir l'accès au "contrat conclu avec la firme israélienne NSO Group pour résoudre certaines enquêtes".

Le 22 septembre 2021, Fedpol refuse l'accès au document en invoquant, entre autres, l'intérêt public à la sécurité intérieure et extérieure de la Suisse.

Saisi par une requête de médiation, le Préposé fédéral à la protection des données et à la transparence recommande à Fedpol de renseigner l'avocat sur l'existence ou l'inexistence d'un contrat conclu avec l'entreprise NSO Group et, le cas échéant, d'y accorder l'accès.

Fedpol formalise sa décision de refus le 15 février 2022 contre laquelle l'avocat interjette recours par-devant le Tribunal administratif fédéral (TAF).

Le TAF rejette le recours, estimant que les exceptions prévues à l'art. 7 al. 1 let. b et c LTrans sont applicables.

L'avocat interjette recours par-devant le Tribunal fédéral et conclut à ce que Fedpol le renseigne sur l'existence d'un contrat avec l'entreprise israélienne et sa transmission le cas échéant en application de la LTrans.

En droit

Les programmes dits “GovWare” (*Government Software*) sont des logiciels informatiques déployés dans le cadre de mesures de surveillance secrètes prévues par l’art. 269ter CPP. Ces mesures répondent à des conditions strictes (cf. art. 269ter al. 1 CPP). Elles sont notamment limitées à certaines infractions pénales (cf. art. 269 al. 2 CPP) et doivent être autorisées par une autorité judiciaire indépendante (cf. art. 274 CPP).

Les logiciels “GovWare” sont utilisés dans le cadre de ces mesures de surveillance afin d’intercepter et de transférer le contenu des communications et les données secondaires de télécommunication sous une forme non cryptée.

Ces programmes sont soumis aux exigences de l’art. 269quater CPP. Ils doivent générer un procès-verbal complet et non modifiable de la surveillance et assurer que le transfert des données du système informatique à l’autorité de poursuite pénale est sécurisé (art. 269quater al. 1 et 2 CPP).

Selon l’art. 6 LTrans, toute personne a, sans avoir à justifier d’un intérêt particulier, le droit de consulter des documents officiels et d’obtenir des renseignements sur leur contenu de la part des autorités. Ce droit d’accès permet de renforcer la confiance des citoyens en leurs institutions et de mieux contrôler l’administration (ATF 150 II 191). Il n’est toutefois pas absolu et les exceptions de l’art. 7 LTrans permettent de limiter l’accès aux documents si les intérêts au maintien du secret l’emportent sur l’intérêt à la transparence.

Entrave à l’exécution de mesures d’autorité

L’accès à un document officiel peut ainsi être restreint, différé ou refusé lorsqu’il entrave l’exécution de mesures concrètes prises par une autorité conformément à ses objectifs (art. 7 al. 1 let. b LTrans).

Cette disposition a pour objectif de protéger la confidentialité d’informations lorsqu’elles servent à la préparation de mesures concrètes d’une autorité, notamment en matière de mesures de surveillance (ATF 144 II 77, consid. 4.3). L’information visée par l’exception n’a pas besoin de porter sur un cas précis ou concret et elle peut aussi, dans certaines situations, découler des pratiques d’une autorité ou de l’identité de ses représentants (BSK BGÖ-STEIMEN, art. 7 LTrans, N 20).

Le TAF retient que la divulgation de l’existence d’un contrat portant sur une catégorie de logiciel espion permettrait à divers individus d’acquérir, avec une haute vraisemblance, une vue d’ensemble sur les possibilités techniques et les limites du logiciel de surveillance. En outre,

la divulgation de l'information demandée par le requérant pourrait permettre l'introduction de programmes malveillants par les cercles visés par ces mesures.

Le recourant soutient, quant à lui, que le refus opposé à sa demande tendrait à soustraire tout marché public de logiciel de surveillance au principe de la transparence. De plus, l'accès à l'éventuel contrat ne devrait pas permettre d'accéder à des informations techniques sur le logiciel.

Le Tribunal fédéral retient – sans justifier ses hypothèses – que l'accès au document pourrait mettre en lumière d'éventuels nouveaux développements techniques. La divulgation de l'information demandée pourrait ainsi rendre inopérantes les tentatives de surveillance ultérieures.

Partant, l'exception de l'art. 7 al. 1 let. b LTrans s'applique.

Sécurité intérieure ou extérieure de la Suisse

Le droit d'accès peut également être limité, différé ou refusé lorsque l'accès à un document risque de compromettre la sûreté intérieure ou extérieure de la Suisse (art. 7 al. 1 let. c LTrans).

Cette exception vise entre autres les activités policières et de renseignements (FF 2003 1851 ch. 2.2.2.1.3). La doctrine retient un risque de mise en péril de la sûreté intérieure ou extérieure lorsque la divulgation d'un document ou d'une information emporte un risque élevé d'attaque (BSK BGÖ-STEIMEN, art. 7 LTrans, N 22).

Pour le TAF, il existe un risque que les personnes ciblées par les mesures de surveillance puissent s'y soustraire ou exploiter d'éventuelles failles du logiciel dont l'accès confirmerait, le cas échéant, l'utilisation en Suisse. Dans cette hypothèse, les autorités de poursuites pénales n'auraient plus cet instrument à disposition.

Le recourant soutient que les personnes susceptibles de tirer profit d'éventuelles failles sont déjà informées de l'utilisation du logiciel Pegasus en raison de la large couverture médiatique dont ce sujet fait l'objet depuis l'été 2021.

Le Tribunal fédéral déduit de l'argumentation du recourant qu'il invoque l'intérêt public à des mesures de surveillances conformes aux droits fondamentaux des individus visés. Il existe, selon notre Cour Suprême, un intérêt public important à reconnaître si les autorités suisses

ont accès au logiciel Pegasus. Elle fait référence à l'utilisation de ce logiciel comme outil de piratage et de surveillance visant des journalistes, avocats, responsables politiques et militants des droits humains au sein d'Etats du Conseil de l'Europe. Le Tribunal fédéral considère toutefois que les statistiques publiées par le Service de Surveillance par poste et télécommunication (SCPT) contribuent à assurer une "certaine information" au public. Ces statistiques reflètent une augmentation de l'utilisation de GovWare à hauteur de 12 fois en 2024 (contre 9 en 2023). Il est également intéressant de relever que les logiciels ont été utilisés pour la poursuite d'infractions de la loi fédérale sur les stupéfiants (75%) et l'infraction d'organisations criminelles et terroristes de l'art. 260ter CP (25%).

Dans la mesure où le recourant n'indique pas dans quelle mesure le cadre procédural suisse ne permet pas une utilisation des GovWare licite et proportionnée, l'exception de l'art. 7 al. 1 let. c LTrans s'applique également.

Partant, le recours est rejeté.

Note

À notre sens, le Tribunal fédéral adopte une approche particulièrement rigoureuse à l'égard de l'argumentation du recourant, sans toutefois prendre en considération la difficulté intrinsèque de la démarche entreprise, laquelle consiste pour ce dernier à solliciter l'accès à un document dont l'existence même doit lui demeurer inconnue le temps de la procédure.

Il nous paraît en outre regrettable que notre Haute Cour ne précise pas davantage les éléments techniques concrets permettant d'apprécier la réalité et l'ampleur des risques invoqués à l'appui du refus d'accès.

Proposition de citation : Mallorie Ashton-Lomax, Les mesures de surveillance secrètes à l'aune de la LTrans, 18 décembre 2025 *in* www.swissprivacy.law/386