Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Décision confirmée par le TF par arrêt du 01.09.2025 (1C_105/2024)

Cour I
A-1310/2022

Arrêt du 9 janvier 2024

Composition

Jérôme Candrian (président du collège),
Jürg Marcel Tiefenthal, Christine Ackermann, juges,
Sébastien Gaeschlin, greffier

Parties

Maître A._____, avocat,
recourant,

contre

Office fédéral de la police (fedpol),
Guisanplatz 1a, 3003 Berne,
autorité inférieure.

Objet

Principe de la transparence ; demande de renseignement relative à l'existence d'un contrat.

Faits :

A.
Dans le sillage d'une enquête menée par un consortium de médias internationaux ayant révélé l'utilisation par plusieurs Etats, parfois de manière abusive, du logiciel « Pegasus », développé par la société israélienne NSO Group, la Radio Télévision Suisse (RTS) a indiqué, dans un article publié en ligne le 11 août 2021, que les autorités de poursuite pénale suisses et le Service de renseignement de la Confédération (ci-après : le SRC) utilisaient un « logiciel espion israélien pour résoudre certaines enquêtes ». Selon l'article, la police fédérale avait indiqué à la RTS que, pour des raisons de protection des tactiques d'enquête et selon les modalités contractuelles, elle ne pouvait donner aucun détail sur la technologie utilisée.

B.
B.a Le 15 août 2021, Maître A._____ (ci-après aussi : le requérant) a déposé auprès de l'Office fédéral de la police (ci-après : fedpol) une demande fondée sur la loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans, RS 152.3) visant à obtenir l'accès au « contrat conclu avec la firme israélienne NSO Group pour l'utilisation de tout logiciel développé par cette firme ».

B.b Le 22 septembre 2021, fedpol a indiqué au requérant ne pas pouvoir donner suite à sa demande de renseignements quant à un éventuel contrat conclu avec des sociétés fournissant des logiciels de surveillance de type *GovWare* (« *Government Software* »), plusieurs intérêts publics, dont la sécurité intérieure et extérieure de la Suisse, y faisant obstacle.

B.c Le 12 octobre 2021, le requérant a déposé une demande en médiation auprès du Préposé fédéral à la protection des données et à la transparence (ci-après : le Préposé fédéral). Il a souligné qu'il existait un intérêt public manifeste à savoir si la Confédération et les cantons utilisaient ou non pour leurs investigations le logiciel espion Pegasus, soit le principal logiciel de surveillance au monde ayant généré une surveillance secrète d'une ampleur inégalée et qui, selon Amnesty International, avait été utilisé pour favoriser des atteintes aux droits humains.

B.d Après que le Préposé fédéral l'ait informé qu'il avait décidé de procéder par écrit, le requérant a déposé des déterminations complémentaires le 6 décembre 2021 en concluant à ce qu'un accès complet au contrat conclu avec la firme israélienne NSO Group lui soit accordé.

B.e Par recommandation du 25 janvier 2022, le Préposé fédéral a recommandé à fedpol de renseigner le requérant sur l'existence ou l'inexistence d'un éventuel contrat conclu avec la firme NSO Group, et, si un tel contrat devait exister, d'y accorder l'accès en application de la loi sur la transparence.

Pour l'essentiel, le Préposé fédéral, a retenu, à titre liminaire, que fedpol n'avait pas indiqué de quelle manière la disposition spéciale de l'art. 67 de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens, RS 121) dont il se prévalait lui était également applicable, ni pourquoi le fait d'informer sur l'existence ou l'inexistence d'un éventuel contrat serait constitutif de l'exception de cette disposition. En outre, fedpol s'était contenté de soulever des motifs d'exception à la transparence sans démontrer de manière factuelle, précise et complète, les raisons concrètes pour lesquelles les conditions relatives à ces exceptions étaient remplies dans le cas d'espèce.

C.
Par décision du 15 février 2022 et en dérogation à la recommandation du Préposé fédéral, fedpol a refusé l'accès aux informations et documents demandés en invoquant plusieurs exceptions au principe de la transparence. En substance, il a considéré, sous l'angle de l'art. 7 al. 1 let. b et c LTrans, que la divulgation des renseignements et des documents sollicités, qui portaient sur des informations critiques pour les intérêts sécuritaires de la Suisse, serait de nature à compromettre gravement la poursuite pénale de personnes soupçonnées d'avoir commis des crimes graves. Par ailleurs, les éventuels contrats avec des fournisseurs de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication contenaient des clauses de confidentialité, ce qui signifiait que la protection des secrets d'affaires ou de fabrication (cf. art. 7 al. 1 let. g LTrans), de même que la politique extérieure et la réputation internationale de la Suisse (cf. art. 7 al. 1 let. d LTrans) – qui concluait ces contrats avec des interlocuteurs étrangers, souvent des entreprises paraétatiques –, faisaient également obstacle à une publication de ces informations, sans leur accord.

D.
D.a Par acte du 18 mars 2021, Maître A._____ (ci-après : le recourant) a interjeté recours contre cette décision auprès du Tribunal administratif fédéral (ci-après aussi : le Tribunal). Il a conclu, avec suite de frais et dépens, à ce que la décision attaquée soit annulée et à ce que fedpol (ci-après : l'autorité inférieure) le renseigne sur l'existence ou l'inexistence

d’un éventuel contrat avec la firme NSO Group et, si un tel contrat devait exister, lui en accorde l’accès.

Pour l’essentiel, le recourant a contesté la réalisation des exceptions au principe de la transparence invoquées par l’autorité inférieure. L’argumentation de l’autorité inférieure à cet égard était, selon lui, insuffisante, car trop générale et se basait sur des assertions non démontrées. Or, il existait un intérêt public manifeste à savoir si la Confédération ou les cantons faisaient usage du logiciel espion Pegasus ou d’un autre logiciel de l’entreprise NSO Group pour leurs investigations, notamment dans la mesure où les droits fondamentaux des personnes surveillées étaient en cause.

D.b Le 23 mai 2022, l’autorité inférieure a déposé sa réponse en précisant sa motivation sous l’angle des exceptions au principe de la transparence. Finalement, elle a fait valoir que l’intérêt public ne pouvait pas consister à savoir quel logiciel de surveillance de la correspondance par télécommunication serait utilisé en Suisse, mais plutôt à s’assurer qu’il serait utilisé conformément aux prescriptions légales strictes, ce qui relevait du contrôle effectué par les tribunaux.

Avec son mémoire de réponse, l’autorité inférieure a transmis au Tribunal un rapport explicatif confidentiel, ainsi que des annexes, destiné à son usage exclusif et qui ne devait pas être porté à la connaissance du recourant en raison d’intérêts prépondérants au maintien du secret.

D.c Par réplique du 22 juin 2022, le recourant s’est notamment prévalu d’une violation de son droit d’être entendu du fait que l’autorité inférieure avait déposé, avec sa réponse, un rapport officiel et des annexes à la seule attention du Tribunal. Sur le fond, il a contesté l’argumentation de l’autorité inférieure résultant de sa réponse.

D.d Le 22 septembre 2022, le recourant a produit à la cause un rapport en anglais du Haut-Commissariat des Nations-Unies aux droits de l’homme (HCDH) sur le thème du droit à la vie privée à l’ère du numérique, qui examine notamment l’utilisation abusive d’outils de piratage intrusifs (« logiciels espions ») par les autorités publiques.

D.e Dans sa duplique du 13 décembre 2022, l’autorité inférieure s’est opposée à ce que le recourant puisse consulter le rapport officiel confidentiel et ses annexes qu’elle avait présentés au Tribunal avec sa réponse, ce qui viderait l’objet du litige en faveur du recourant.

Elle a également fait valoir que le document du HCDH, produit par le recourant, et son écriture du 22 septembre 2022 ne contenaient pas d'éléments nouveaux pertinents et a conclu à ce qu'ils ne soient pas admis en cause.

D.f Le 15 décembre 2022, le recourant a produit une étude sollicitée par la Commission d'enquête du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (commission PEGA), intitulée « *The use of Pegasus and equivalent surveillance spyware* ».

D.g Par écriture spontanée du 4 janvier 2023, l'autorité inférieure a conclu à ce que l'étude susmentionnée ne soit, elle non plus, pas admise en cause, dans la mesure où son contenu n'aurait pas de lien avec l'objet du litige, soit avec la question de savoir si fedpol avait – ou non – conclu un contrat avec NSO Group.

D.h Dans ses observations finales du 20 janvier 2023, le recourant s'est, à nouveau, plaint d'une violation de son droit d'être entendu et a soutenu qu'il était inexact de prétendre que les enquêtes diligentées sur le plan international relatives au logiciel Pegasus n'avaient aucune pertinence pour l'examen d'une requête de transparence. Il a par ailleurs produit une autre étude demandée par la Commission PEGA du Parlement européen, intitulée « L'incidence de Pegasus sur les droits fondamentaux et les processus démocratiques », en précisant que ses conclusions étaient alarmantes.

D.i Par courriers du 20 juin 2023, du 3 octobre 2023 et du 15 novembre 2023, auxquels il a été donné réponse respectivement le 22 juin 2023, le 9 octobre 2023 et le 21 novembre 2023, le recourant s'est enquis auprès du Tribunal de l'état d'avancement de la procédure de recours.

Les autres faits et arguments pertinents des parties seront repris et examinés, en tant que de besoin, dans les considérants en droit qui suivent.

Droit :

1.

La procédure de recours est régie par la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA, RS 172.021), à moins que la loi du 17 juin 2005 sur le Tribunal administratif fédéral (LTAF, RS 173.32) ou les dispositions spéciales consacrées par la législation matérielle applicable,

ici la LTrans et l'ordonnance du 24 mai 2006 sur le principe de la transparence dans l'administration (ordonnance sur la transparence [OTrans, RS 152.31]), n'en disposent autrement (cf. art. 37 LTAF, ég. art. 16 al. 1 LTrans).

Le Tribunal examine d'office et librement sa compétence (cf. art. 7 PA) et la recevabilité des recours qui lui sont soumis.

1.1 Sous réserve des exceptions figurant à l'art. 32 LTAF – non pertinentes en l'espèce –, le Tribunal administratif fédéral connaît, en vertu de l'art. 31 LTAF, des recours contre les décisions au sens de l'art. 5 PA prises par les autorités mentionnées à l'art. 33 LTAF. En l'espèce, fedpol étant une autorité précédente au sens de l'art. 33 let. d LTAF (cf. annexe 1 de l'ordonnance sur l'organisation du gouvernement et de l'administration du 25 novembre 1998 [OLOGA, RS 172.010.1] par renvoi de l'art. 8 al. 1 let. a), et l'acte attaqué satisfaisant aux conditions qui prévalent à la reconnaissance d'une décision au sens de l'art. 5 al. 1 PA, le Tribunal est compétent pour connaître du présent litige.

1.2 Pour le surplus, déposé en temps utile (art. 50 al. 1 PA) et en la forme requise (art. 52 PA), par le destinataire de la décision litigieuse, laquelle a participé à la procédure devant l'autorité inférieure et possède un intérêt digne de protection à son annulation ou à sa modification (art. 48 al. 1 PA), le recours est recevable, de sorte qu'il convient d'entrer en matière.

2.

2.1 En sa qualité d'autorité de recours, le Tribunal dispose d'une pleine cognition. Il revoit librement l'application du droit par l'autorité inférieure (art. 49 PA), y compris l'excès ou l'abus du pouvoir d'appréciation (let. a), la constatation des faits (let. b) et l'opportunité de la décision attaquée (let. c), tous griefs que le recourant peut soulever à l'appui de son recours. Conformément à la maxime inquisitoire, le Tribunal vérifie d'office les faits constatés par l'autorité inférieure (art. 12 PA), sous réserve du devoir de collaborer des parties (art. 13 PA).

Le Tribunal applique le droit d'office, sans être lié par les motifs invoqués (cf. art. 62 al. 4 PA), ni par l'argumentation juridique développée dans la décision entreprise. Il se limite en principe aux griefs soulevés et n'examine les questions de droit non invoquées que dans la mesure où les arguments des parties ou le dossier l'y incitent (cf. ATF 135 I 91 consid. 2.1 ; ATAF 2014/24 consid. 2.2, 2012/23 consid. 4).

2.2 L'objet du présent litige consiste à examiner le bien-fondé de la décision de l'autorité inférieure, par laquelle elle a refusé totalement l'accès à des renseignements et à des documents en relation avec l'existence ou non, le cas échéant avec le contenu, d'un contrat avec la société NSO Group portant sur l'acquisition de logiciels espions.

Dans les considérants qui suivent, il s'agira d'examiner préalablement les questions formelles posées par la présente procédure, soit le respect du droit d'être entendu du recourant en lien avec la production, par l'autorité inférieure, d'un rapport confidentiel à l'attention exclusive du Tribunal, d'une part (cf. *infra* consid. 4), et le droit du recourant de produire des pièces qu'il estime pertinentes pour la résolution du litige, d'autre part (cf. *infra* consid. 5). Après avoir rappelé les principes essentiels gouvernant les demandes d'accès aux documents officiels fondées sur la législation sur la transparence (cf. *infra* consid. 6), il conviendra ensuite de déterminer si les exceptions au principe de la transparence invoquées par l'autorité inférieure à l'appui de sa décision sont réalisées ou non (cf. *infra* consid. 7 et 8), au regard également du principe de la proportionnalité (cf. *infra* consid. 10). Enfin, le recourant se référant aux activités du SRC, il conviendra de signaler que l'application éventuelle de la LRens ferait aussi obstacle au principe de la transparence en l'espèce (cf. *infra* consid. 11).

3.
Avant toutes choses, le cadre légal régissant l'utilisation de logiciels espions, tels que celui objet de la présente demande d'accès et de renseignements, peut être précisé de la manière suivante.

3.1 Dans le contexte des mesures de surveillance secrètes qui peuvent être ordonnées dans le cadre de la procédure pénale, l'art. 269*ter* du Code de procédure pénale du 5 octobre 2007 (CPP, RS 312.0), entré en vigueur le 1er mars 2018, permet, à certaines conditions strictes et pour un catalogue restreint d'infractions pénales (cf. art. 269*ter* al. 1 let. b CPP et art. 286 al. 2 CPP), la mise en œuvre de « programmes informatiques spéciaux de surveillance de la correspondance par télécommunication » dans un système informatique (ordinateur, tablette numérique, téléphone portable), soit essentiellement l'installation de logiciels espions dans le but d'intercepter et de transférer le contenu des communications et les données secondaires de télécommunication sous une forme non cryptée. L'on parle de « *Government Software* », abrégé « *Govware* », également souvent improprement appelés « chevaux de Troie » (« *Staatstrojaner* »). En effet, outre le fait que – à la différence du cheval de Troie –, le *GovWare* est utilisé dans un but légal, à savoir lutter contre la criminalité, l'objectif

n’est pas que le programme considéré se propage, contrairement à ce qui peut être le cas d’un cheval de Troie, mais de permettre au ministère public de surveiller un appareil considéré, respectivement une personne (cf. Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication [Message LSCPT] du 27 février 2013, FF 2013 2379, p. 2466 s. ; HANSJAKOB, Was ist GovWare?, in*:* Jusletter du 11 septembre 2017).

Il s’agit d’une mesure de surveillance de la correspondance particulière, utilisée avant tout pour lire et écouter des communications chiffrées de bout-en-bout, qui ne requiert pas la collaboration d’un fournisseur de services de télécommunication ou du Service Surveillance de la correspondance par poste et télécommunication (Service SCPT). Les art. 269 à 279 CPP s’appliquent également au recours à la surveillance par *GovWare*, sauf si et dans la mesure où les art. 269*ter* et *quater* CPP prévoient des règles spéciales. L’introduction de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication dans un système informatique est ordonnée par le ministère public, puis autorisée par une autorité judiciaire indépendante, le tribunal des mesures de contrainte (cf. art. 274 CPP, contrôle *a priori*). Après la communication de la surveillance, la personne concernée peut recourir devant le tribunal cantonal (cf. art. 279 et art. 393 ss CPP, contrôle *a posteriori*).

3.2 Les *GovWare* sont un mode de surveillance dont la nature est particulièrement intrusive, et qui permet *techniquement* d’accéder à l’intégralité des informations privées, soit des données potentiellement intimes, enregistrées dans un système informatique, bien que *juridiquement* la perquisition en ligne d’un système informatique au moyen de *GovWare* soit exclue, tout comme l’utilisation au moyen d’un *GovWare* de la caméra ou du micro d’un ordinateur, à tout le moins dans un autre but que la surveillance de la correspondance par télécommunication (cf. Message LSCPT, p. 2466 s., 2471 s. ; HANSJAKOB, Einsatz von GovWare zulässig oder nicht ? : zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie, Jusletter du 1er novembre 2011, n° 646 ; SYLVAIN MÉTILLE, Commentaire romand Code de procédure pénale suisse, 2ème éd. 2019, n° 13 et 20 ad art. 269*ter* CPP).

Fedpol met à disposition les *GovWare*, administre les licences et maintient le système et le support aux cantons en servant de point de contact unique avec le fabricant. Le rapport explicatif de la révision de l'ordonnance sur les émoluments pour les décisions et les prestations de l'Office fédéral de

la police (ordonnance sur les émoluments de fedpol [OEmol-fedpol, RS 172.043.60], datant de février 2019, précisait ce qui suit :

> « par l'arrêté fédéral du 11 mars 2015, le Parlement a voté un crédit global de 99 millions de francs affecté au programme. Une partie de ce dernier relève de l'acquisition de programmes informatiques spéciaux (projet P4-GovWare), lesquels doivent permettre aux autorités de poursuite pénale de surveiller la correspondance par télécommunication de suspects recourant à des moyens cryptés. L'utilisation de programmes informatiques spéciaux se fonde sur l'art. 269*ter* du code de procédure pénale (CPP). […] fedpol a évalué ces programmes informatiques pour pouvoir effectuer ses propres tâches d'enquête et à la demande des cantons (projet P4-GovWare) et armasuisse a acquis ces programmes sur mandat de fedpol ».

3.3 L'art. 269*quate*r CPP pose des exigences auxquelles doivent répondre les programmes informatiques spéciaux de surveillance de la correspondance par télécommunication en vue de garantir l'authenticité des preuves obtenues, ainsi que la sécurité des données. Les programmes informatiques spéciaux de surveillance de la correspondance par télécommunication doivent notamment générer un procès-verbal complet et non modifiable de la surveillance (al. 1) et assurer que le transfert des données du système informatique à l'autorité de poursuite pénale compétente soit sécurisé (al. 2). Selon les statistiques du Service SCPT, les programmes informatiques spéciaux au sens de l'art. 269*ter* CPP ont été utilisés 7 fois en 2022 et 11 fois en 2021 (cf. https://www.li.admin.ch/fr/stats).

3.4 En outre, le SRC peut également, à certaines conditions strictes et après avoir obtenu l'autorisation du Tribunal de céans, ainsi que l'aval du chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS), utiliser des programmes informatiques spéciaux en tant que mesure de recherche soumise à autorisation (cf. art. 26 al. 1 LRens), en présence d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse, que constituent notamment les activités terroristes ou l'espionnage, ou lorsque la sauvegarde d'autres intérêts nationaux importants le requiert (cf. en particulier art. 27 *cum* 19 al. 2 let. a à d ou art. 3 LRens).

4.

Dans sa réplique et ses observations finales, le recourant a conclu à ce que l'accès au rapport confidentiel, ainsi qu'à ses annexes, lesquels ont été produits par l'autorité inférieure au cours de la présente procédure de recours à l'attention du Tribunal uniquement (cf. *supra* Etat de fait, let. D.b),

lui soit accordé. Il s'est prévalu d'une violation de son droit d'être entendu à cet égard, grief qu'il convient d'examiner au préalable.

4.1 En procédure administrative fédérale, le droit d'être entendu au sens de l'art. 29 PA comprend en particulier le droit pour la partie concernée par une procédure pendante de prendre connaissance du dossier de l'autorité. Ce droit est concrétisé aux art. 26 à 28 PA. Quant à son étendue, le droit de consulter le dossier au sens de l'art. 26 PA porte sur toutes les pièces relatives à la procédure sur lesquelles la décision est susceptible de se fonder (cf. ATF 133 I 100 consid. 4.3 à 4.6, arrêt du Tribunal fédéral [TF] 1C_674/2013 du 12 décembre 2013 consid. 2.2 ; ATAF 2014/38 consid. 7, ATAF 2013/23 consid. 6.4.1, arrêt du Tribunal administratif fédéral [TAF] C-1507/2015 du 10 juin 2016 consid. 3.3.2). Ce droit n'est cependant pas absolu. Au sens de l'art. 27 al. 1 PA, l'autorité ne peut refuser la consultation des pièces que si : des intérêts publics importants de la Confédération ou des cantons, en particulier la sécurité intérieure ou extérieure de la Confédération, exigent que le secret soit gardé (let. a) ; des intérêts privés importants, en particulier ceux de parties adverses, exigent que le secret soit gardé (let. b) ; l'intérêt d'une enquête officielle non encore close l'exige (let. c). Selon le deuxième alinéa de cette disposition, le refus d'autoriser la consultation des pièces ne peut s'étendre qu'à celles qu'il y a lieu de garder secrètes. Aux termes de l'art. 28 PA, une pièce dont la consultation a été refusée à la partie ne peut être utilisée à son désavantage que si l'autorité lui en a communiqué, oralement ou par écrit, le contenu essentiel se rapportant à l'affaire et lui a donné en outre l'occasion de s'exprimer et de fournir des contre-preuves.

4.2

4.2.1 En l'occurrence, le Tribunal observe que le rapport confidentiel en cause, de même que ses annexes contiennent précisément des informations que le recourant souhaite obtenir par sa demande d'accès en vertu de la loi sur la transparence ; elles vont même, à certains égards, au-delà. Or la réserve des intérêts publics posée à l'art. 27 al. 1 let. a PA se recouvre avec les exceptions à la transparence posées par l'art. 7 al. 1 let. a à f LTrans. L'autorité inférieure se prévalant d'intérêts publics importants pour la sécurité intérieure et extérieure de la Confédération pour justifier le refus d'accès au rapport officiel et à ses annexes (cf. *infra* consid. 8 et 9), lesquels sont également protégés par l'art. 27 al. 1 let. a PA (cf. ADRIEN RAMELET, Le droit de consulter le dossier en procédure administrative, pénale et civile : Etude comparative de droit fédéral, Berne 2021, N 424 ss et réf. citées), remettre ces documents au recourant en cours de procédure au titre du droit de consulter le dossier viderait ainsi cette dernière de sa

substance matérielle, de sorte qu'il est justifié de ne pas lui en permettre la consultation sous l'angle du droit procédural (cf. arrêts du TAF A-4729/2020 du 24 novembre 2022 consid. 5.3.3, A-2630/2020 du 17 février 2022 consid. 7, A-3349/2018 du 19 juin 2019 consid. 4, A-2569/2018 du 4 juin 2019 consid. 2.4).

4.2.2 Par ailleurs, le recourant s'est vu communiquer le contenu essentiel du rapport officiel se rapportant à l'affaire et il a eu l'occasion de s'exprimer et de fournir des contre-preuves. En particulier, la réponse de l'autorité inférieure au recours datée du 23 mai 2022, sur laquelle le recourant a pu se déterminer, comporte les éléments déterminants sur la base desquels elle a fondé sa décision, de même que les éléments déterminants pour l'issue de la présente procédure de recours. Les arguments du recourant soulevés dans le cadre de sa réplique démontrent au demeurant qu'il a parfaitement compris l'essentiel de l'argumentation de l'autorité inférieure fondant le refus d'accès.

4.3 Il s'ensuit qu'il n'y a pas lieu de donner suite à la requête du recourant tendant à la consultation des documents transmis par l'autorité inférieure à l'attention du Tribunal uniquement. Le grief de violation du droit d'être entendu s'avère mal fondé.

5.
Il y a ensuite lieu de se déterminer sur les conclusions de l'autorité inférieure tendant à ce que les documents produits par le recourant au cours de la procédure de recours, soit essentiellement des rapports relatifs à l'utilisation de logiciels espions, en particulier Pegasus, ne soient pas versés au dossier de la cause.

5.1 L'autorité inférieure soutient pour l'essentiel que les documents produits ne contiennent pas d'éléments nouveaux et pertinents pour l'issue du présent litige. En effet, dans la mesure où ils ne font pas mention des raisons pour lesquelles le recourant devrait avoir accès ou non aux informations et aux éventuels documents demandés, les documents produits ne seraient pas décisifs et ne devraient pas être pris en compte.

5.2
5.2.1 À teneur de l'art. 33 al. 1 PA, l'autorité admet les moyens de preuve offerts par la partie s'ils paraissent propres à élucider les faits. Le droit d'être entendu, tel qu'il est garanti par cette disposition de même que par l'art. 29 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst., RS 101), comprend notamment le droit de produire des

preuves quant aux faits de nature à influer sur la décision, d'obtenir qu'il soit donné suite à ses offres de preuves pertinentes, de participer à l'administration des preuves essentielles ou à tout le moins de s'exprimer sur son résultat, lorsque cela s'avère susceptible d'influer sur la décision à rendre (cf. ATF 148 II 73 consid. 7.3.1, 145 I 167 consid. 4.1, 143 V 71 consid. 4.1 et les réf. cit.)

5.2.2 À cela s'ajoute qu'en vertu de l'art. 32 PA, l'autorité apprécie, avant de prendre la décision, tous les allégués importants qu'une partie a avancés en temps utile (al. 1). Elle peut prendre en considération des allégués tardifs s'ils paraissent décisifs (al. 2). En conséquence, les parties disposent également de la possibilité de modifier leur position juridique durant la procédure, de présenter de nouveaux éléments de fait connus ou non jusque-là, qui se sont déroulés avant ou seulement pendant la procédure de recours, ou de nouveaux moyens de preuve ou éléments de motivation (cf. arrêt du TF 2C_95/2019 du 13 mai 2019 consid. 3.2 ; ATAF 2010/53 consid. 15.1 ; PATRICK SUTTER, in: Christoph Auer/Markus Müller/Benjamin Schindler [éd.], Kommentar zum Bundesgesetz über das Verwaltungsverfahren [VwVG], Zurich/St-Gall 2008, art. 32 n° 10). Le caractère décisif des allégués tardifs des parties s'examine à la lumière de l'exigence d'un établissement complet et exact des faits pertinents conforme à la maxime inquisitoire, mais aussi du principe de l'application correcte du droit (cf. WALDMANN/BICKEL, in : Praxiskommentar zum VwVG., art. 32 n° 14). La maxime inquisitoire, qui prévaut en particulier en droit public (cf. ATF 140 I 285 consid. 6.3.1), notamment devant le Tribunal de céans (cf. *supra* consid. 2.1), oblige notamment les autorités compétentes à prendre en considération d'office l'ensemble des pièces pertinentes qui ont été versées au dossier (cf. arrêts du TF 2C_633/2018 du 13 février 2019 consid. 5.1.1 et 2C_207/2017 du 2 novembre 2017 consid. 3.1).

5.3 En l'occurrence, au vu des règles qui viennent d'être rappelées, le Tribunal ne discerne pas de motifs pour lesquels il conviendrait d'écarter du dossier de la présente procédure les pièces produites par le recourant, d'autant moins que leur pertinence ne saurait d'emblée être exclue dans le cadre d'une procédure relative à l'application de la LTrans. Dès lors, en effet, que le recourant souhaite obtenir des renseignements relatifs à l'existence ou l'inexistence d'un éventuel contrat conclu avec la société NSO Group, qui a développé et commercialisé le logiciel Pegasus, les documents produits par le recourant peuvent permettre de mieux appréhender les intérêts au maintien du secret, respectivement l'intérêt public à la transparence, dont les parties se prévalent de part et d'autre.

6.
Il s'agit à présent de rappeler le cadre légal général applicable en matière de transparence dans l'administration.

6.1 La LTrans vise à promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration fédérale. À cette fin, elle contribue à l'information du public en garantissant l'accès aux documents officiels (art. 1 LTrans). Ce droit d'accès général concrétise le but essentiel de la loi, qui est de renverser le principe du secret de l'activité de l'administration au profit de celui de transparence (cf. ATF 144 II 77 consid. 5.1, 142 II 340 consid. 2.2, 142 II 324 consid. 3.4 ; arrêt du TF 1C_462/2018 du 17 avril 2019 consid. 3.2 ; ATAF 2016/18 consid. 4.1, 2014/24 consid. 3.1). Il s'agit, en effet, de rendre le processus décisionnel de l'administration plus transparent dans le but de susciter la confiance du citoyen en l'administration et en son fonctionnement, de renforcer le caractère démocratique des institutions publiques, tout en améliorant le contrôle des autorités étatiques (cf. ATF 147 I 47 consid. 3.5 et les réf. cit., 136 II 399 consid. 2.1 ; ATAF 2011/52 consid. 3).

6.2 Ainsi, pour autant que la LTrans soit applicable à raison de la personne et de la matière (cf. art. 2 et 3 LTrans) et qu'aucune disposition spéciale au sens de l'art. 4 LTrans n'existe qui fasse exception à son application (à ce sujet voir le 30ème rapport d'activité 2022/2023 du Préposé fédéral, p. 80-81, qui dresse une liste des dispositions spéciales réservées au sens de l'art. 4 LTrans, disponible sur internet), toute personne a le droit de consulter – et de demander une copie sous réserve des droits d'auteur – des documents officiels (cf. art. 5 LTrans) et d'obtenir des renseignements sur leur contenu de la part des autorités (art. 6 al. 1 et al. 2 LTrans), sans devoir justifier d'un intérêt particulier (cf. ATF 142 II 340 consid. 2.2, 133 II 209 consid. 2.1).

La LTrans fonde donc une *présomption* en faveur du libre accès aux documents officiels (cf. ATF 142 II 340 consid. 2.2 et les réf. citées). Dès lors, si l'autorité décide de limiter ou refuser l'accès à des documents officiels, elle supporte le fardeau de la preuve destiné à renverser la présomption du libre accès aux documents officiels, instituée par la LTrans. En d'autres termes, elle doit exposer pour quel motif et dans quelle mesure une ou plusieurs des exceptions légales figurant aux art. 7 et 8 LTrans est ou sont réalisées (cf. ATF 142 II 324 consid.3.4 ; ATAF 2014/24 consid. 3, 2011/52 consid. 6 ; Message du Conseil fédéral relatif à loi fédérale sur la transparence [Message LTrans], FF 2003 1807ss, 1844 ; PASCAL MAHON/OLIVIER GONIN in: Stephan C. Brunner/Luzius Mader [éd.], Öffentlichkeitsgesetz,

Handkommentar, Berne 2008 [ci-après : Öffentlichkeitsgesetz], ad art. 6 n° 11). À cet égard, ses explications doivent être convaincantes, à savoir être précises et claires, complètes et cohérentes (cf. arrêts du TAF A-2564/2018 du 5 août 2020 consid. 4.5.1, A-2352/2017 du 11 décembre 2019 consid. 4.3, A-3884/2017 du 6 septembre 2018 consid. 3.3.1 et A-6/2015 du 26 juillet 2017 consid. 4.1).

6.3 Dans les cas spécifiés à l'art. 7 al. 1 LTrans, l'accès aux documents officiels est restreint, différé ou refusé.

6.3.1 Les intérêts publics (let. a à f) ou privés (let. g et h) énoncés à l'art. 7 al. 1 LTrans, qui peuvent justifier le maintien du secret, doivent alors revêtir un caractère prépondérant par rapport à l'intérêt (public) à l'accès auxdits documents, respectivement à la transparence. La loi procède par avance à une pesée des intérêts en cause, dans la mesure où elle énumère de manière exhaustive les différents cas où les intérêts publics ou privés apparaissent prépondérants (cf. not. ATF 144 II 77 consid. 3 et les réf. cit. ; ATAF 2014/24 consid. 3.4 ; arrêt du TAF A-2022/2021 du 7 juin 2022 consid. 4.4.1 et les réf. cit.).

6.3.2 Cela étant, il revient ensuite à l'autorité d'examiner de cas en cas si les exceptions légales sont réalisées. En effet, pour que les clauses d'exclusion figurant à l'art. 7 al. 1 LTrans trouvent application, il faut que l'éventuel préjudice consécutif à la divulgation atteigne une certaine intensité et que le risque de sa survenance, selon le cours ordinaire des choses, soit hautement probable (cf. ATAF 2013/50 consid. 8.1, ATAF 2011/52 consid. 6 ; URS STEIMEN, in: Maurer-Lambrou/Blechta [éd.], Basler Kommentar Datenschutzgesetz, Öffentlichkeitsgesetz, 3 éd., 2014 [BSK DSG/BGÖ], ad art. 7 LTrans n° 4 ; COTTIER/SCHWEIZER/WIDMER, in: Öffentlichkeitsgesetz, ad art. 7 n° 4). Une conséquence mineure ou simplement désagréable engendrée par l'accès ne saurait constituer une telle atteinte (cf. ATF 144 II 77 consid. 3 et les réf. cit., 142 II 340 consid. 2.2, 133 II 209 consid. 2.3.3). L'atteinte menaçante doit être importante. Si sa survenance ne doit pas apparaître comme certaine, cette atteinte ou menace ne saurait uniquement être imaginable ou possible, au risque de vider de son sens le changement de paradigme introduit par la LTrans (cf. ATF 142 II 324 consid. 3.4 ; arrêt du TAF A-1751/2017 du 1er mai 2020 consid. 8.3).

Comme en général en matière de limitation des droits fondamentaux, ces clauses d'exclusion doivent être interprétées restrictivement (cf. arrêts du TAF A-1751/2017 du 1er mai 2020 consid. 8.3, A-3649/2014 du 25 janvier 2016 consid. 8.2.1, A-700/2015 du 26 mai 2015 consid. 4.2 et les réf. cit.).

Dans tous les cas, en application du principe de la proportionnalité (cf. art. 5 al. 2 Cst.), lorsqu'une limitation paraît justifiée, l'autorité doit choisir la variante la moins incisive et qui porte le moins possible atteinte au principe de la transparence (cf. ATF 142 II 324 consid. 3.3, 142 II 313 consid. 3.6 ; ATAF 2013/50 consid. 9.3 ; arrêts du TAF A-6475/2017 du 6 août 2018 consid. 3.2.2 ; A-3367/2017 du 3 avril 2018 consid. 3.4). Ainsi, l'accès ne peut pas simplement être refusé lorsque le document exigé contient des informations qui ne sont pas accessibles selon le catalogue d'exceptions de l'art. 7 LTrans. Dans ce cas, il convient plutôt – et autant que possible – de le restreindre, à savoir garantir un accès partiel aux informations du document, ceci par l'anonymisation, le caviardage, la publication partielle ou l'ajournement (cf. ATF 142 II 324 consid. 3.3, 142 II 313 consid. 3.6 ; arrêts du TAF A-2564/2018 précité consid. 4.5.8, A-6475/2017 précité consid. 3.2.2 ; URS STEIMEN, in: BSK DSG/BGÖ, ad art. 7 LTrans N 9 ss.).

6.3.3 Comme cela ressort de ce qui précède, le mécanisme de protection des intérêts au maintien du secret prévu par la LTrans repose sur l'existence ou l'inexistence d'un risque de préjudice, et non – à l'exception de l'art. 7 al. 2 LTrans – sur une véritable pesée des intérêts de l'administration au maintien du secret, d'une part, et du requérant à l'accès aux documents demandés, d'autre part. Lorsque les autorités doivent escompter un risque sérieux qu'un préjudice d'une certaine intensité se produise, le document doit être tenu secret, indépendamment de la légitimité des raisons pour lesquelles le demandeur sollicite l'accès à l'information (cf. arrêt A-700/2015 précité consid. 4.2 et les réf. cit.).

7.

Sur ce vu, il convient en premier chef d'examiner si la divulgation des informations et documents demandés par le recourant tomberait, comme le fait valoir l'autorité inférieure, sous le coup de l'exception de l'art. 7 al. 1 let. b LTrans.

7.1

7.1.1 Au terme de cette disposition, le droit d'accès est limité, différé ou refusé lorsque l'accès à un document officiel peut avoir pour effet d'entraver l'exécution de mesures concrètes prises par une autorité conformément à ses objectifs. L'art. 7 al. 1 let. b LTrans garantit que des informations puissent être gardées secrètes lorsqu'elles servent à la préparation de mesures concrètes d'une autorité, notamment en matière de mesures de surveillance, d'inspections des autorités fiscales ou de certaines campagnes d'information (cf. ATF 144 II 77 consid. 4.3 ; Message LTrans, FF 2003 1807 ss, 1850 ch. 2.2.2.1.2). Selon la jurisprudence, les enquêtes, les

inspections et le contrôle administratif visant à garantir que les citoyens respectent la loi sont protégés par cette disposition (cf. arrêt du TAF A-4781/2019 consid. 5.4.1 et réf. cit.). Cette exception peut donc être invoquée lorsque, avec une grande probabilité, une mesure n'atteindrait plus ou pas entièrement son but si certaines informations qui préparent cette mesure étaient rendues accessibles (cf. Message LTrans, p. 1850 ch. 2.2.2.1.2 ; pour un développement complet de la question, voir arrêt du TAF A-683/2016 du 20 octobre 2016 consid. 5.4). Le maintien du secret de l'information doit être vu comme la clé de la bonne exécution de la mesure envisagée (cf. Message LTrans 1807ss, 1850 ch. 2.2.2.1.2 ; arrêts du TAF A-3334/2019 du 3 novembre 2020, A-4571/2015 du 10 août 2016 consid. 6.1 et les réf. cit.). Cela dit, la loi n'exige pas, comme le prévoyait encore le projet (cf. Message LTrans, 1807 ss, 1850 ch. 2.2.2.1.2), une entrave « considérable », dans la mesure où cette exigence a été supprimée lors des débats parlementaires (cf. BO 2004 N 1261 s. et BO 2004 p. 593).

7.1.2 L'information en question, si elle doit entraver l'exécution de mesures concrètes, ne doit pas nécessairement concerner un cas particulier et concret (*einzelfallbezogen*). Elle peut, dans certaines circonstances, avoir pour objet la pratique d'une autorité (cf. arrêt du TAF A-683/2016 précité consid. 5.4.1 ; URS STEIMEN, in: BSK DSG/BGÖ, ad art. 7 LTrans n° 20). Toutefois, l'accomplissement de tâches générales ou l'activité de surveillance d'une autorité dans son ensemble ne sont pas couverts par cette disposition (cf. ATF 144 II 77 consid. 4.2 s. ; not. arrêt du TAF A-4781/2019 précité du 17 juin 2020 consid. 5.4.3 et les réf. cit.).

7.2

7.2.1 L'autorité inférieure soutient que, si le public avait accès à des informations et à des documents sur le type et le mode de fonctionnement d'un *GovWare* qui serait utilisé – ou non – en Suisse, la poursuite pénale s'en verrait gravement et lourdement péjorée. La divulgation de l'existence d'un type précis de logiciel espion révélerait l'utilisation finale du système concerné, ainsi que ses possibilités et ses limites. Les criminels pourraient alors se rabattre spécifiquement sur des moyens de communication échappant à toute surveillance. Ils pourraient aussi déployer en amont des outils et des mécanismes de détection pour reconnaître le *GovWare* utilisé. En somme, l'autorité inférieure relève que les tâches des autorités chargées de la poursuite pénale et l'efficacité de leur action dans la lutte contre la criminalité doivent faire l'objet d'une protection de tous les instants. Or, l'information et les documents demandés tomberaient dans la catégorie des informations qui doivent bénéficier d'une protection accrue et ne peuvent

être divulguées, afin de ne pas porter préjudice aux intérêts des autorités devant accomplir les missions qui leur sont dévolues de par la loi.

7.2.2 Le recourant oppose en substance à l'autorité inférieure qu'un accord portant sur l'acquisition d'un *spyware*, aussi complexe et détaillé soit-il, n'est pas supposé renfermer des informations techniques sur l'utilisation, les mécanismes ou la mise en place du programme informatique en question. Il n'est pas non plus censé donner des précisions sur les données des personnes cibles ou l'utilisation concrète du logiciel. D'ailleurs, le recourant précise qu'il ne demande pas à ce que le type ou le mode de fonctionnement du *GovWare* soient divulgués, et encore moins à ce que des mesures secrètes soient annoncées, mais bien l'accès à un document permettant de déterminer si les autorités suisses ont accès à un logiciel espion précis et controversé. Or, la connaissance de l'existence même d'un *GovWare* ne saurait entraver l'action publique ou empêcher les autorités d'en faire usage. Au surplus, il fait valoir que les personnes prévoyant de commettre ou ayant commis un crime justifiant le recours à la surveillance au moyen d'un *GovWare* – soit une mesure qui doit être qualifiée d'*ultima ratio* –, prennent déjà les mesures leur permettant de se prémunir d'intrusion dans leurs systèmes. Dites mesures sont d'ailleurs précisées dans un récent rapport du Conseil de l'Europe (« Le logiciel espion Pegasus et ses répercussions sur les droits de l'homme », juin 2022), qu'il produit en cause en version anglaise.

À cet égard, le recourant rappelle que le litige revêt une importance médiatique et que les controverses à l'endroit de la société NSO Group sont multiples. Selon lui, l'autorité inférieure doit faire preuve de plus de transparence à l'aune de l'ampleur du scandale suscité par le logiciel Pegasus, un programme qui a été utilisé à des fins dolosives et qui représente une menace pour la démocratie. Le recourant met également l'accent sur les risques que pourrait comporter le recours à un logiciel comme Pegasus, notamment du point de vue de la sécurité des données, en arguant qu'il pourrait contenir une *back-door* et permettre à son concepteur, comme certains le prétendent, d'avoir accès aux données résultant de la surveillance par les autorités.

7.3 De l'avis de la Cour de céans, l'autorité inférieure peut être suivie lorsqu'elle affirme que la divulgation au public de l'existence d'un type spécifique de logiciel espion utilisé dans le cadre de la poursuite pénale et dans le domaine du renseignement permettrait, avec un haut degré de vraisemblance, à divers cercles d'acquérir une vue d'ensemble sur les

possibilités techniques offertes par cette mesure de surveillance, ainsi que ses limites.

7.3.1 Les personnes susceptibles d'être concernées par la surveillance par *GovWare* pourraient ainsi chercher à y échapper, notamment en adoptant certains comportements afin de réduire le risque d'être infecté ou en érigeant des sécurités et des barrières informatiques idoines. De fait, pour être installé, le *GovWare* utilise généralement une porte dérobée ou une faille de sécurité de l'appareil visé ou d'un logiciel présent sur ledit appareil. Il peut être installé physiquement ou à distance. L'installation à distance implique généralement une action de la personne visée comme l'acceptation de mises à jour, l'ouverture d'un courriel et d'un lien de téléchargement (masqué), etc. (cf. SYLVAIN MÉTILLE, op. cit., n° 26 ad art. 269*ter* CPP). Le *GovWare* doit souvent être conçu en fonction de l'environnement dans lequel il doit être installé et de sa configuration précise, ainsi que de son but. Il ne s'agit pas d'un produit standard, mais d'un outil sur mesure, qui doit être configuré et adapté en fonction de l'appareil visé, et qui est particulièrement onéreux (cf. Message LSCPT, FF 2013 2469 ; UMBERTO PAJAROLA/THOMAS JAKOB, Kommentar zur Schweizerischen Strafprozessordnung [StPO], Donatsch/Lieber/Summers/Wohlers [éd.] 3ème éd. 2020, art. 269*ter* n° 10s. et 17s.). Il va de soi que, pour atteindre son but, le déploiement du *GovWare* doit avoir lieu à l'insu du détenteur du système informatique considéré.

7.3.2 Certes, comme le fait valoir le recourant, diverses mesures, pour certaines élémentaires, permettant de réduire les risques d'infection par un *GovWare* sont connues. Il n'en demeure pas moins que d'autres mesures de protection pourraient dépendre du type de logiciel utilisé et de son fonctionnement, dans la mesure où chaque type de logiciel espion a ses spécificités et ses limites. La divulgation d'un type spécifique de *GovWare* utilisé – ou non – en Suisse semble, de l'avis du Tribunal, d'autant plus problématique qu'il résulte de sources publiques que, en l'état actuel de la technique, seul un type de programme informatique de surveillance de la communication chiffrée était utilisé dans notre pays en 2019 (cf. Rapport explicatif de la révision de l'OEmol-fedpol, février 2019) et que le nombre de *GoWare* disponibles sur le marché soit (très) limité.

7.3.3 À cela s'ajoute que l'utilisation de *GovWare* n'est pas sans risque. Les failles de sécurité créées ou exploitées par le logiciel peuvent, le cas échéant, être utilisées par des criminels pour introduire des programmes malveillants. Par ailleurs, selon les compétences techniques de la personne cible ou des personnes auxquelles elle fait appel, il serait également

moins complexe de détecter la présence du logiciel, dont les caractéristiques seraient par hypothèse connues, dans un ordinateur. Or, si le *GovWare* est démasqué, il peut être analysé, voire modifié, par des spécialistes qui, à leur tour, pourraient l'utiliser de manière abusive (cf. PAJAROLA/JAKOB, op. cit., art. 269*ter* n° 20). Ce risque ne saurait être toléré. Le recourant semble d'ailleurs admettre sa possible survenance lorsqu'il précise que le fonctionnement du logiciel Pegasus – ce qui, du reste, pourrait valoir pour d'autres logiciels également –, a été largement commenté et qu'une société genevoise a même développé un outil permettant de détecter les traces de sa présence sur un téléphone ou un autre appareil.

7.3.4 Sur ce vu, il y a lieu de retenir que la connaissance par le public de l'utilisation ou non d'un certain type de *GovWare* en Suisse serait susceptible, avec un haut degré de probabilité, de remettre en cause l'efficacité d'une mesure de surveillance de la correspondance par télécommunication prévue par la loi et utilisée pour des investigations portant sur des infractions ou des menaces particulièrement graves. Or, ce mode de surveillance est essentiel au vu de l'utilisation toujours plus croissante de la téléphonie et/ou autre communication par Internet ; les données communiquées et interceptées dans ce contexte sont en effet souvent chiffrées et resteraient donc illisibles ou inutilisables sans l'utilisation de *GovWare* (cf. Message LSCPT, FF 2013 2467 ; PAJAROLA/JAKOB, op. cit., art. 269*ter* n° 2 ss. ; THOMAS HANSJAKOB, Was ist GovWare?, in: Jusletter 11 septembre 2017, n° 7).

7.4 En définitive, le Tribunal retient qu'il existe suffisamment d'éléments permettant de considérer que le maintien du secret quant au(x) type(s) de logiciel(s) espion(s) utilisé(s) en Suisse constitue la clé de la bonne exécution de la mesure de surveillance par *GovWare*, de sorte que l'exception au principe de la transparence de l'art. 7 al. 1 let. b LTrans est réalisée.

8.
À l'appui de la décision attaquée, l'autorité inférieure se prévaut en outre de l'exception au droit d'accès consacrée à l'art. 7 al. 1 let. c LTrans.

8.1 Selon cette disposition, le droit d'accès peut être limité, différé ou refusé, lorsque l'accès à un document officiel risque de compromettre la sûreté intérieure ou extérieure de la Suisse. L'art. 7 al. 1 let. c LTrans vise essentiellement à protéger les activités policières, douanières, de renseignement et militaires. Cela étant, ce n'est pas tant la nature des activités des autorités impliquées qui est décisive, mais bien la nature des intérêts et des biens juridiques menacés. Cette exception au principe de la

transparence permet de maintenir secrète toute information propre à mettre en danger la sécurité publique si elle était diffusée. La sécurité intérieure ou extérieure de la Suisse peut être compromise par des attaques ou des menaces, telles que notamment la criminalité de manière générale, l'extrémisme violent, le terrorisme ou l'espionnage (STEIMEN, op. cit., art. 7 n° 21 ; cf. aussi COTTIER/SCHWEIZER/WIDMER, op. cit., art. 7 n° 27). Peuvent par exemple tomber sous le coup de cette disposition, des informations sur l'organisation, l'activité ou la stratégie des autorités, en particulier celles qui assument des tâches relevant de la sécurité (cf. STEIMEN, op. cit., art. 7 n° 22). Toutefois, même à des fins légitimes de sécurité, il convient d'examiner avec soin si la divulgation des documents demandés pourrait mettre sérieusement en danger la sécurité publique (cf. arrêts du TAF A-700/2015 précité consid. 6.1 et A-1177/2014 du 2 février 2015 consid. 4.2.1, avec les réf. cit.).

8.2 Comme déjà esquissé, il existe un lien étroit entre l'atteinte sérieuse et prévisible à l'efficacité de la mesure de surveillance par *GovWare* pour le cas où la demande d'accès du recourant devait être admise, d'une part, et l'efficacité de la poursuite pénale, de même que des investigations menées par le SRC, d'autre part. Contrairement à ce que fait valoir le recourant, sa demande d'accès ne porte pas sur la question de savoir si la Suisse utilise, de manière générale, des logiciels espions mais permettrait de déterminer si les autorités ont recours à un type spécifique de *GovWare*. Or, si les personnes cibles pouvaient, d'une manière ou d'une autre, se soustraire à la surveillance ordonnée, voire si le logiciel espion en cause – ou les failles de sécurité exploitées ou crées – pouvait être utilisé à des fins malveillantes par des tiers, les autorités de poursuite pénale et le SRC seraient privées d'un instrument efficace et essentiel dans la lutte contre la criminalité, respectivement dans la détection précoce et la prévention de menaces pour la sécurité de la Suisse. Par suite, il sied de retenir que l'accès aux informations et aux éventuels documents demandés représenterait également une menace sérieuse pour la sécurité intérieure, de sorte que le maintien du secret se justifie également à ce titre (cf. art. 7 al. 1 let. c LTrans).

9.

Dès lors que les exceptions consacrées par l'art. 7 al. 1 let. b et c LTrans trouvent application au cas d'espèce (cf. *supra* consid. 7 et 8), la question de la réalisation des autres exceptions au droit d'accès invoquées par l'autorité inférieure, à savoir l'art. 7 al. 1 let. d et g LTrans, peut demeurer ouverte.

10.
Vu le bien-fondé des exceptions au principe de la transparence ainsi reconnu, qui s'oppose à l'information du recourant quant à l'existence ou non d'un contrat portant sur un tel logiciel, la question d'un accès partiel à un tel document ne se pose pas. Il convient toutefois de préciser ce qui suit au titre du principe de la proportionnalité (cf. *supra* consid. 6.3).

10.1 Le Tribunal souligne avoir conscience que, compte tenu des révélations, et du scandale qui s'en est suivi, au sujet du logiciel Pegasus, développé par la société israélienne NSO Group, et dont de nombreux Etats ont fait l'acquisition, et qui a, dans certains d'entre eux, été détourné pour cibler des défenseurs des droits humains, des opposants politiques, des journalistes, des avocats, des diplomates et des chefs d'Etats (à ce sujet voir not. le rapport de l'Assemblée parlementaire du Conseil de l'Europe, « Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'Etat » du 20 septembre 2023 [Doc. 15825] ; l'enquête menée par la commission PEGA qui a abouti à l'adoption d'une recommandation par le Parlement européen le 15 juin 2023 ; le « Report A/HRC/51/17 of the Office of the United Nations High Commissioner for Human Rights [OHCHR], The right to privacy in the digital age » du 4 août 2022), l'intérêt public à la transparence, qui consiste notamment à savoir si ledit logiciel est à la disposition des autorités suisses, est important. D'autant plus que le recours à des *GovWare* est une mesure très intrusive du point de vue des droits fondamentaux, bien plus qu'une mesure classique de surveillance de la correspondance par télécommunication, et que le logiciel Pegasus pourrait, à certains égards, différer des outils d'interception « traditionnels » utilisés par les autorités répressives (cf. à ce sujet Contrôleur européen de la protection des données [CEPD], «Remarques préliminaires sur les logiciels espions modernes», 15 février 2022, p. 3-4).

10.2 Cela étant, il peut d'abord être relevé que le recours aux programmes de surveillance de type *GovWare* est strictement encadré en droit suisse, notamment dans la mesure où il n'est permis qu'en présence de soupçons suffisants laissant présumer une infraction ou une menace pour la sécurité de la Suisse figurant dans un catalogue exhaustif et limitatif et qu'il fait l'objet d'un contrôle judiciaire indépendant quant au respect des conditions strictes posées par la loi, qui inclut un contrôle de sa proportionnalité et du respect de l'exigence d'une double subsidiarité (cf. aussi ci-avant consid. 3.1 et 3.4). Du reste, comme on l'a vu (cf. *supra* consid. 3.3), les ministères publics cantonaux et fédéral tiennent une statistique annuelle des surveillances au moyen d'un *GovWare,* qui indique notamment le type d'infraction, et qui doit être transmise au Service SCPT, lequel publie chaque

année une statistique consolidée (cf. art. 269*ter* al. 4 CPP et art. 13 de l'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (OSCPT, RS 780.11), ce qui contribue à assurer une certaine information du public.

10.3 Il convient ensuite de rappeler que le Tribunal de céans a déjà eu l'occasion de se prononcer sur l'accès à des documents officiels détenus par le Service SCPT portant sur les divers logiciels utilisés dans le cadre de la surveillance de la correspondance par poste et télécommunication (cf. arrêt A-700/2015 du 26 mai 2015 consid. 5.7, déjà cité). Le Tribunal avait, à l'époque, déjà confirmé le refus d'accès *complet* aux informations et aux documents sollicités, également sur le fondement de l'art. 7 al. 1 let. b et c LTrans, vu le risque que leur divulgation représentait pour l'efficacité de l'action pénale.

Ainsi, et pour autant que les documents sollicités existent, le Tribunal considère, pour les raisons précédemment exposées, qu'une divulgation partielle, sous une forme caviardée, ne s'imposerait pas au regard du principe de proportionnalité (cf. *supra* consid. 6.3). De fait, la seule confirmation ou infirmation de l'existence d'un contrat avec NSO Group permettrait, avec un grand degré de probabilité, aux criminels ou à des personnes représentant une menace pour la sécurité de la Suisse, potentiellement hautement spécialisés, de tirer des conclusions sur le type de *GovWare* utilisé en Suisse, ce qui serait de nature à porter une atteinte grave à l'efficacité de cette mesure de surveillance, pourtant considérée comme indispensable par le législateur à la lutte contre la criminalité au vu de l'évolution technique dans le domaine des télécommunications.

11.
Enfin, le recourant se référant aux activités du SRC, il convient de préciser qu'en toute hypothèse, l'art. 67 LRens ferait déjà en soi obstacle au droit d'accès prétendu.

11.1 Le recourant signale en particulier l'interpellation du Conseiller national Carlo Sommaruga du 18 septembre 2019 (19.5518), libellée en ces termes :

> « Citizen Lab, laboratoire de l'Université de Toronto spécialisé dans la recherche sur les menaces numériques pour la société civile, rapporte l'utilisation à grande échelle de la technologie malveillante Pegasus de la société de logiciels espions NSO Group par des gouvernements et des particuliers visant la surveillance du trafic de courriels

> et des téléphones portables des défenseurs des droits humains. - Le Conseil fédéral est-il au courant de ce mode d'espionnage ? - Que fait-il contre cela ? ».

Et la réponse du Conseil fédéral du 23 septembre 2019 :

> « Le Conseil fédéral sait que des gouvernements et des privés sont en mesure d'utiliser de tels outils techniques pour acquérir illégalement des informations sur le territoire suisse. L'entreprise NSO Group commercialise un service nommé Pegasus, qui permet d'infiltrer des téléphones portables en exploitant des failles ou des faiblesses de leurs logiciels. Ce sujet a notamment été évoqué dans le premier rapport semestriel Melani de 2017. Les services de renseignement utilisent fréquemment les technologies de l'information et de la communication pour acquérir des informations. Ils ont de plus en plus recours aux outils "cyber" parallèlement aux techniques classiques comme le recrutement de sources humaines. Dans le cadre de sa mission légale, le Service de renseignement de la Confédération (SRC) décèle et prévient les activités d'espionnage contre les intérêts suisses. Il transmet le résultat de ses recherches aux autorités de poursuite pénale, à qui il revient, le cas échéant d'ouvrir une enquête contre les auteurs présumés. »

Or, le recourant considère qu'il y a un risque réel d'espionnage par ce biais des citoyens suisses et des forces de sécurité, ce qui impose d'exiger un contrôle démocratique par le biais du principe de la transparence.

11.2 L'art. 67 LRens, qui prévoit que la loi sur la transparence ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations au sens de la LRens, constitue une disposition spéciale réservée par une loi fédérale au sens de l'art. 4 let. a LTrans (cf. not. recommandation du Préposé fédéral du 10 décembre 2018 : X. und Y. – Nachrichtendienst des Bundes [NDB] / Genehmigungspflichtige Beschaffungsmassnahmen). L'art. 4 let. a LTrans réserve les dispositions spéciales d'autres lois fédérales qui déclarent certaines informations secrètes. Une disposition spéciale peut ainsi empêcher l'accès à un document officiel ou le soumettre à des règles divergentes, qui peuvent être plus strictes ou, au contraire, faciliter la consultation du document. Or, selon une très récente recommandation du Préposé fédéral dans une autre affaire, qui faisait suite à une demande d'accès portant sur quatre catégories de documents touchant aux *GovWare* à disposition du SRC, il a été retenu que l'argumentation de cette dernière autorité, selon laquelle la liste des *GovWare* utilisés en Suisse et de leur fabricant pouvait donner des indications sur les méthodes de recherche d'informations du SRC, pouvait être suivie. De l'avis du Préposé fédéral, cette liste permettait de faire des déductions suffisamment concrètes sur la façon de procéder et de travailler du SRC dans la

recherche d'informations, soit dans le domaine que le législateur a exclu de la LTrans (cf. art. 67 LRens ; recommandation du Préposé fédéral du 20 septembre 2023 X. – NDB / Informationen zu GovWare und zum Austausch mit GovWare-Anbietenden).

11.3 En l'espèce, dans la mesure où les informations et les documents demandés pourraient, le cas échéant, révéler l'utilisation d'un type spécifique de programme informatique de surveillance de la correspondance par télécommunication en Suisse, lequel serait susceptible d'être utilisé également par le SRC, la question de l'application de l'art. 67 LRens, qui exclut celle de la LTrans aux documents portant sur la recherche d'informations du SRC, pourrait se poser (cf. *supra* consid. 3.4). Contrairement à l'argumentation du Préposé fédéral dans sa recommandation du 25 janvier 2022 en la présente affaire, qui a retenu que « fedpol n'a[vait] pas indiqué dans son argumentaire de quelle manière l'art. 67 LRens, qui règle l'activité du SRC, lui était également applicable », seule la nature du document en cause et les informations qu'il comporte est décisive, indépendamment de l'autorité qui le détient (cf. dans ce sens not. : 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). Ainsi, la question de savoir si un contrat a ou non été conclu avec une entreprise déterminée pour faire l'acquisition d'un type spécifique de logiciel espion tomberait, en toute hypothèse, sous le coup de l'exception consacrée à l'art. 67 LRens, car la connaissance de cette information pourrait mettre en danger les mesures prises par la Suisse en cas de menace concrète pour sa sécurité intérieure et extérieure.

12.
De l'ensemble des considérants qui précèdent, il suit que l'autorité inférieure n'a pas enfreint le droit en refusant la demande d'accès du recourant aux renseignements et aux éventuels documents litigieux.

Par conséquent, le recours, mal fondé, doit être rejeté et la décision attaquée confirmée.

13.
Demeure la question des frais et dépens.

13.1 Vu l'issue de la procédure, il y a lieu de mettre les frais à la charge du recourant, conformément à l'art. 63 al. 1 PA en relation avec le règlement du 21 février 2008 concernant les frais, dépens et indemnités fixés par le Tribunal administratif fédéral (FITAF, RS 173.320.2). Ceux-ci seront fixés

à 1‘000 francs et prélevés sur l’avance de frais déjà versée du même montant.

13.2 Le recourant, qui succombe, n’a pas droit à des dépens (art. 64 al. 1 PA et art. 7 al. 1 FITAF *a contrario*). L’autorité inférieure n’y a elle-même pas droit (cf. art. 7 al. 3 FITAF).

(le dispositif est porté en page suivante)

Par ces motifs, le Tribunal administratif fédéral prononce :

1.
Le recours est rejeté.

2.
Les frais de procédure de 1’000 francs sont mis à la charge du recourant. Cette somme est prélevée sur l’avance de frais déjà versée du même montant.

3.
Il n’est pas alloué de dépens.

4.
Le présent arrêt est adressé au recourant, à l'autorité inférieure, au Secrétariat général du Département fédéral de justice et police (DFJP) et au Préposé fédéral.

L'indication des voies de droit se trouve à la page suivante.

Le président du collège : Le greffier :

Jérôme Candrian Sébastien Gaeschlin

Indication des voies de droit :

La présente décision peut être attaquée devant le Tribunal fédéral, 1000 Lausanne 14, par la voie du recours en matière de droit public, dans les trente jours qui suivent la notification (art. 82 ss, 90 ss et 100 LTF). Ce délai est réputé observé si les mémoires sont remis au plus tard le dernier jour du délai, soit au Tribunal fédéral soit, à l'attention de ce dernier, à La Poste Suisse ou à une représentation diplomatique ou consulaire suisse (art. 48 al. 1 LTF). Le mémoire doit être rédigé dans une langue officielle, indiquer les conclusions, les motifs et les moyens de preuve, et être signé. La décision attaquée et les moyens de preuve doivent être joints au mémoire, pour autant qu'ils soient en mains de la partie recourante (art. 42 LTF).

Expédition :

Le présent arrêt est adressé :

– à la recourante (acte judiciaire)
– à l'autorité inférieure (courrier recommandé)
– au Secrétariat général du DFJP (acte judiciaire)
– au Préposé fédéral