BGer 1C_105/2024 vom 1. September 2025

Bundesgericht, 2025-09-01, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/bger_1C_105_2024

FR: TF 1C_105/2024 du 1 septembre 2025

IT: TF 1C_105/2024 del 1 settembre 2025

Erwägungen

E. 1

L'arrêt attaqué, relatif à l'accès à un document au sens de la LTrans, constitue une décision finale (art. 90 LTF) rendue par le Tribunal administratif fédéral (art. 86 al. 1 let. a LTF) dans une cause de droit public (art. 82 let. a LTF).

E. 1.1

Selon l' art. 83 let. a LTF , le recours est irrecevable contre les décisions concernant la sûreté intérieure ou extérieure du pays, la neutralité, la protection diplomatique et les autres affaires relevant des relations extérieures, à moins que le droit international ne confère un droit à ce que la cause soit jugée par un tribunal. Quand bien même l'instance précédente a reconnu que l'accès requis représenterait aussi une menace sérieuse pour la sécurité intérieure au sens de l' art. 7 al. 1 let . c LTrans, le motif d'irrecevabilité n'est pas applicable en l'espèce, dans la mesure où la décision contestée n'est pas un acte ayant un caractère politique prépondérant, au sens d'un "acte de gouvernement" classique (ATF 137 I 371 consid. 1.2; arrêts 1C_214/2023 et 1C_228/2023 du 5 mars 2025 consid. 1.2 et les références citées). En conclusion, aucune des exceptions prévues à l' art. 83 LTF n'est réalisée, si bien que la voie du recours en matière de droit public est ouverte.

E. 1.2

Le recourant, qui a pris part à la procédure devant l'autorité précédente (art. 89 al. 1 let. a LTF), est particulièrement touché par l'arrêt attaqué qui confirme le refus de sa demande de renseignement relative à l'existence d'un contrat; il dispose ainsi d'un intérêt digne de protection à l'annulation ou à la modification de l'arrêt attaqué (art. 89 al. 1 LTF).

E. 1.3

Le recourant met en doute la capacité de la Cheffe

ad interim du domaine de direction "Prévention de la criminalité et droit" de représenter fedpol et de signer la réponse au recours. L'art. 12 de la directive de fedpol sur la réglementation des droits de signature (fondée sur l'art. 49 al. 1 let. a de la loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997 [LOGA; RS 172.010] et sur la directive du DFJP pour la délégation de l'autorisation de signature du chef de département du 1er février 2012) donne compétence de décision et de signature au Chef/à la Cheffe du domaine de direction "Prévention de la criminalité et droit" quand le destinataire est un des tribunaux fédéraux. Fedpol explique que la Cheffe suppléante dudit domaine était devenue Cheffe

ad interim à cette date (en raison de la vacance du poste de Chef/de la Cheffe) et était par conséquent habilitée à signer la réponse au recours. Il n'y a pas lieu de mettre en doute cette explication, ce que le recourant ne parvient d'ailleurs pas à faire.

E. 1.4

Les autres conditions de recevabilité sont au surplus réunies, si bien qu'il y a lieu d'entrer en matière sur le recours.

E. 2

Avec sa réponse au recours devant le Tribunal fédéral, l'intimé a transmis le rapport officiel confidentiel qu'il avait produit devant l'instance précédente. Invoquant "notamment le droit à un procès équitable" (art. 6 par. 1 CEDH), le recourant sollicite que ce rapport - destiné au seul usage du Tribunal fédéral - lui soit adressé pour consultation.

Selon l' art. 56 LTF , les parties ont le droit notamment de prendre connaissance des pièces produites (al. 1), une restriction à ce droit n'étant admissible que pour la sauvegarde d'intérêts prépondérants, et moyennant communication du contenu essentiel des éléments sur lesquels le tribunal entend se fonder (al. 2 et 3).

En l'espèce, le rapport confidentiel en question ainsi que ses annexes contiennent précisément des informations auxquelles le recourant demande accès en se fondant sur la loi sur la transparence. Certaines informations vont même sous certains aspects au-delà. La réserve d'intérêts prépondérants de l' art. 56 al. 2 LTF se recoupe avec les exceptions à la transparence posées par l'art. 7 al. 1 let. a à f LTrans. Remettre ces documents au recourant en cours de procédure au titre du droit de consulter le dossier viderait celle-ci de sa substance, fedpol 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. Il est par conséquent justifié de ne pas autoriser la consultation durant la présente procédure.

Au demeurant, le recourant s'est vu communiquer le contenu essentiel du rapport officiel se rapportant à l'affaire et a eu l'occasion de s'exprimer et de fournir des contre-preuves. Il a compris l'essentiel de l'argumentation de l'intimé motivant le refus d'accès.

E. 3

Dans sa réplique, sans véritablement formuler de grief, le recourant reproche au TAF de lui avoir refusé l'accès au rapport confidentiel du 23 mai 2022. Il fait aussi valoir des éléments nouveaux dont le fait que fedpol a acheté des produits de la société D._____; il produit des pièces y relatives.

Selon la jurisprudence, le droit de réplique déduit des art. 6 CEDH et 29 al. 2 Cst. n'a pas vocation à permettre à la partie recourante de présenter ainsi au Tribunal fédéral des critiques nouvelles ou des griefs qui auraient déjà pu figurer dans l'acte de recours (cf. ATF 143 II 283 consid. 1.2.3; 135 I 19 consid. 2.2; la partie recourante ne saurait, par ce biais, remédier à une motivation défaillante ou encore compléter les motifs de son recours. Admettre le contraire aurait pour conséquence de prolonger le délai légal de recours, ce que prohibe expressément l' art. 47 al. 1 LTF , et de créer des inégalités de traitement. Dans cette mesure, le Tribunal fédéral ne tiendra pas compte des explications et éléments nouveaux présentés au-delà du délai de recours, ceux-ci étant irrecevables (cf. arrêt 1C_240/2024 du 28 avril 2025 consid. 1.2).

Par ailleurs, le recourant n'explique pas en quoi les différentes pièces produites à l'appui de sa réplique résulteraient de l'arrêt attaqué et seraient admissibles devant le Tribunal fédéral à l'aune de l' art. 99 LTF . Il n'en sera par conséquent pas tenu compte.

Au demeurant, le recourant ne démontre pas que les produits de D._____ (utilisés lors de perquisitions et fouilles) permettraient une mesure de surveillance secrète au sens du CPP, comme le logiciel de surveillance de type

GovWare .

E. 4

Dans un grief d'ordre formel qu'il convient d'examiner en premier lieu, le recourant se plaint d'un établissement inexact des faits (art. 97 al. 1 LTF).

E. 4.1

Le Tribunal fédéral statue sur la base des faits établis par l'autorité précédente (art. 105 al. 1 LTF), sous réserve des cas prévus à l' art. 105 al. 2 LTF (ATF 142 I 155 consid. 4.4.3). Le recourant ne peut critiquer les constatations de fait ressortant de la décision attaquée que si celles-ci ont été effectuées en violation du droit au sens de l' art. 95 LTF ou de manière manifestement inexacte, c'est-à-dire arbitraire (sur cette notion, cf. ATF 142 II 355 consid. 6), et si la correction du vice est susceptible d'influer sur le sort de la cause (art. 97 al. 1 LTF), ce que le recourant doit démontrer (art. 106 al. 2 LTF).

E. 4.2

En l'espèce, le recourant reproche à l'instance précédente d'avoir délimité l'objet du litige à la question de savoir si le recourant pouvait être renseigné sur l'existence ou non d'un contrat conclu entre l'intimé et B._____. Se référant à un article paru le 14 août 2021 sur le site Internet du quotidien

Neue Zürcher Zeitung intitulé "

Auch Schweizer Behörden setzten auf Pegasus ", il soutient que l'utilisation du logiciel Pegasus par l'intimé serait "de notoriété publique", si bien qu'il ne s'agirait plus d'un secret. Il prétend que seule la confirmation officielle de l'utilisation du logiciel, par le biais de la procédure de transparence, ferait défaut.

E. 4.2.1

Les faits notoires sont des faits qu'il n'est pas nécessaire d'alléguer ni de prouver et dont l'existence est certaine au point d'emporter la conviction du juge, qu'il s'agisse de faits connus de manière générale du public ou seulement du juge. Pour être notoire, un renseignement ne doit pas être constamment présent à l'esprit; il suffit qu'il puisse être contrôlé par des publications accessibles à chacun. En ce qui concerne les informations figurant sur Internet, le Tribunal fédéral a précisé qu'il y a lieu de retenir que seules les informations bénéficiant d'une "empreinte officielle" (par ex: Office fédéral de la statistique, inscriptions au registre du commerce, cours de change, horaire de train des CFF, etc.) peuvent en principe être considérées comme notoires (ATF 149 I 91 consid. 3.4; 143 IV 380 consid. 1.2). En outre, les publications de médias ne constituent pas des faits notoires, à défaut d'empreinte officielle (arrêt 2C_700/2022 du 25 novembre 2022 consid. 7.6.2).

E. 4.2.2

Le moyen de preuve invoqué par le recourant à l'appui de son allégué est une publication émanant d'un média, sur son site Internet. Il ne s'agit pas d'une source officielle, ce que le recourant admet, dans la mesure où il reconnaît qu'une confirmation officielle de l'usage du logiciel fait encore défaut. Le recourant ne démontre en outre pas que les informations

figurant dans l'article cité seraient, comme il l'avance, de notoriété publique. Au demeurant, si l'utilisation du logiciel Pegasus était véritablement un fait notoire, on peine à comprendre que le recourant persiste à conclure à ce que l'intimé le renseigne sur l'existence ou l'inexistence d'un éventuel contrat conclu avec la firme B._____.

E. 4.2.3

Le même constat s'impose s'agissant d'autres suppositions avancées par le recourant, qui ne ressortent pas de l'arrêt attaqué: il en va ainsi de la prétendue possibilité, pour la société B._____, d'avoir accès aux données de l'intimé et du SRC par le truchement d'une

backdoor implémentée dans le logiciel Pegasus, du nombre de "

GovWare " disponibles sur le marché ou des mesures que les réseaux criminels auraient déjà pu prendre pour contrer le

GovWare Pegasus. Outre le fait qu'il n'étaie pas ses assertions, le recourant n'explique pas en quoi la correction de l'état de fait sur ces points - fût-elle fondée - aurait la moindre influence sur le sort de la cause, se contentant d'affirmer de façon appellatoire que l'intimé craindrait de devoir s'expliquer sur les investigations conduites au moyen d'un "logiciel illégal".

E. 4.3

Par conséquent, le grief d'établissement manifestement inexact des faits doit être écarté dans la mesure de sa recevabilité.

E. 5

Il convient d'abord de définir les logiciels de surveillance tels que celui objet de la présente demande d'accès et de présenter le cadre légal les régissant.

E. 5.1

Dans le contexte des mesures de surveillance secrètes qui peuvent être ordonnées dans le cadre de la procédure pénale, l'art. 269ter 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. 269ter al. 1 let. b CPP et art. 286 al. 2 CPP), la mise en oeuvre 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. On parle de "Government Software", abrégé

GovWare , 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 (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.; Thomas 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).

E. 5.2

L'utilisation de

GovWare n'est possible que dans le cadre d'une procédure pénale et ne peut avoir lieu à titre préventif (Message LSCPT p. 2466). L'introduction de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication dans un système informatique est ordonnée par le ministère public (arrêt 7B_91/2024, 7B_92/2024 du 16 octobre 2024 consid. 4.2.2). Elle doit ensuite être autorisée par une autorité judiciaire indépendante, le tribunal des mesures de contrainte (cf. art. 272 et 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). L'exécution de la mesure incombe à la police: c'est elle qui installe le programme informatique dans le système visé (cf. HANSJAKOB, op. cit., no 659 ad art. 269ter CPP).

Cette mesure de contrainte est soumise aux conditions spéciales énumérées aux lettres a à c de l'alinéa précité: les conditions fixées à l' art. 269 al. 1 et 3 CPP sont remplies (let. a); il s'agit de poursuivre l'une des infractions mentionnées à l' art. 286 al. 2 CPP (let. b); les mesures de surveillance de la correspondance par télécommunication au sens de l' art. 269 CPP prises jusqu'alors sont restées sans succès ou ces mesures n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement difficile (cf. arrêt 7B_91/2024, 7B_92/2024 du 16 octobre 2024 consid. 4.2.1). L'utilisation d'un

GovWare entre en considération lorsque la personne visée (soit la personne prévenue) utilise des moyens de communication chiffrée de bout en bout ("

End-to-End encryption "), le but étant que les autorités puissent contourner ce chiffrement et accéder au contenu des communications cryptées (cf. HANSJAKOB, op. cit., no 603 ad art. 269ter CPP).

E. 5.3

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.; Thomas 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. 269ter CPP).

E. 5.4

L' art. 269quater 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. 269ter CPP ont été utilisés 12 fois en 2024 et 9 fois en 2023 (cf. https://www.li.admin.ch/fr/stats consulté le 18 juin 2025).

E. 6

Le recourant reproche à l'instance précédente d'avoir considéré que le droit d'accès à l'information requise pouvait être refusé en application tant de l' art. 7 al. 1 let. b LTrans que de l' art. 7 al. 1 let . c LTrans.

E. 6.1

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 général concrétise le but fixé à l' art. 1 LTrans , qui est de renverser le principe du secret de l'activité de l'administration au profit de celui de transparence quant à la mission, l'organisation et l'activité du secteur public. Il s'agit en effet de rendre le processus décisionnel de l'administration plus transparent dans le but de renforcer le caractère démocratique des institutions publiques, de même que la confiance des citoyens dans les autorités, tout en améliorant le contrôle de l'administration (ATF 150 II 191 consid. 3 et les références citées).

Conformément à ce but, la loi définit de manière large la notion de documents officiels (art. 5 LTrans), le champ d'application à raison de la personne (art. 2 LTrans) ainsi que les bénéficiaires et les conditions d'exercice du droit d'accès (art. 6 LTrans). La loi s'applique ainsi à l'ensemble de l'administration fédérale (art. 2 al. 1 let. a LTrans), y compris les organismes de droit public ou privé chargés de rendre des décisions.

E. 6.2

L' art. 4 let. a LTrans réserve toutefois 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 (ATF 148 II 16 consid. 3.4.1; 150 II 191 consid. 3). Tel est le cas de l' art. 67 LRens , mentionné par le TAF. Cette disposition prévoit que la LTrans ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations au sens de la LRens (cf. recommandation du Préposé fédéral du 20 septembre 2023, X. - NDB, n

o 17 s.; ANDRÉ WINKLER, Mit Spezialbestimmungen gegen Transparenz, in 10 ans LInf Fribourg, n

o 24 s.; 32e Rapport d'activités 2024/2025 du Préposé fédéral à la protection des données et à la transparence, p. 85).

En l'espèce, fedpol n'expose pas effectuer de la recherche d'informations au sens de la LRens. Il n'explique pas non plus en quoi l' art. 67 LRens lui serait applicable. Il n'y a donc

pas lieu d'appliquer de dispositions spéciales réservées au sens de l' art. 4 let. a LTrans .

E. 6.3

Les art. 7 ss LTrans prévoient en outre des exceptions et restrictions au droit d'accès prévu à l' art. 6 LTrans . Dans les cas spécifiés à l' art. 7 al. 1 LTrans , l'accès aux documents officiels est restreint, différé ou refusé. Le législateur a procédé de manière anticipée à une pondération des intérêts en cause, dans la mesure où il énumère de manière exhaustive les différents cas où les intérêts publics ou privés apparaissent prépondérants par rapport au principe de l'accès. Selon la jurisprudence, l'atteinte aux intérêts publics ou privés protégés par cette disposition ne doit pas apparaître certaine, mais il ne suffit pas non plus qu'elle soit hypothétiquement liée à l'accès aux documents. Elle doit en outre apparaître sérieuse, n'importe quelle conséquence bénigne ou désagréable ne pouvant être assimilée à une atteinte (ATF 144 II 77 consid. 3 et les références citées).

En présence d'une exception au droit d'accès, il convient d'examiner au cas par cas si les intérêts au maintien du secret l'emportent sur l'intérêt à la transparence ou si, cas échéant, en application du principe de proportionnalité (cf. art. 5 al. 2 Cst.), un accès partiel peut être envisagé, par exemple par anonymisation, caviardage, publication partielle ou report dans le temps (ATF 142 II 313 consid. 3.6; 142 II 324 consid. 3.3).

E. 6.4.1

Selon l' art. 7 al. 1 let. b LTrans , le droit d'accès est limité, différé ou refusé lorsque l'accès à un document officiel entrave l'exécution de mesures concrètes prises par une autorité conformément à ses objectifs.

Cette disposition 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). Cette exception peut 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. Le maintien du secret de l'information doit être vu comme la clé de la bonne exécution de la mesure envisagée (cf. Message du Conseil fédéral relatif à la LTrans du 12 février 2003, FF 2003 1850 ch. 2.2.2.1.2). Il ne suffit pas d'une simple possibilité d'entrave de mesures concrètes: le maintien du secret doit apparaître comme une condition au succès de ces mesures (URS STEIMEN, in BSK DSG/BGÖ, 4

e éd. 2024, n

o 19 ad art. 7 LTrans ; cf. ég. sur l'ensemble arrêt 1C_412/2022 du 9 août 2023 consid. 5.1).

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 ou encore, dans des domaines sensibles, l'identité de mandataires de l'autorité (STEIMEN,

op. cit. , N 20 ad art. 7 LTrans). 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.; arrêt 1C_412/2022 du 9 août 2023 consid. 5.1).

E. 6.4.2

En l'espèce, le Tribunal administratif fédéral a considéré qu'il existait 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 constituait 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 était réalisée.

Il a retenu en substance 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 (dont les personnes susceptibles d'être concernées par la surveillance

GovWare) d'acquérir une vue d'ensemble sur les possibilités techniques offertes par cette mesure de surveillance, ainsi que ses limites. L'instance précédente a ajouté que les failles de sécurité créées ou exploitées par un logiciel

GovWare pouvaient, le cas échéant, être utilisées par des criminels pour introduire des programmes malveillants (cf. Pajarola/Jakob, Kommentar zur Schweizerischen Strafprozessordnung [StPO], Donatsch/Lieber/Summers/Wohlers [éd.], 3e éd. 2020, art. 269ter n° 20).

E. 6.4.3

Face à ce raisonnement, le recourant fait uniquement valoir que le refus d'accès tendrait à soustraire tout marché public de logiciel de surveillance au principe de la transparence, ce qui viderait la LTrans de sa substance. Il soutient aussi que les informations et documents qu'il requiert ne devraient pas contenir la moindre information technique sur le logiciel en cause - dont la divulgation entraverait les mesures prises par les autorités de poursuite pénale - puisque le

GovWare est par nature un logiciel sur mesure. Il relève encore que "vu l'engouement médiatique suscité par ce logiciel, l'accès aux documents ne permettrait que de lever ce qui s'apparenterait à un secret de polichinelle": indépendamment des informations sollicitées, les réseaux criminels susceptibles de contrer un tel

GovWare étaient d'ores et déjà susceptibles d'avoir pris des mesures en ce sens.

L'argumentation du recourant repose ainsi uniquement sur des allégations de faits et ne répond que dans une moindre mesure à la motivation de l'arrêt attaqué retenant que le maintien du secret constitue la clé de la bonne exécution de la mesure de surveillance par

GovWare . Quand bien même le public aurait été informé du fonctionnement du logiciel Pegasus et de certaines mesures permettant d'en limiter l'efficacité comme le recourant le prétend, on ne voit pas en quoi ces éléments contrediraient une probable remise en cause de l'efficacité des mesures de surveillance par

GovWare en cas de divulgation de l'utilisation ou non du logiciel. En effet, dans la mesure où les fournisseurs de systèmes informatiques développent des technologies de cryptage toujours plus performantes, il est nécessaire que les logiciels à disposition des autorités soient continuellement améliorés, pour être en mesure de surveiller les systèmes visés. Or la connaissance de l'utilisation d'un logiciel déterminé peut impliquer la connaissance de (nouvelles) spécificités techniques dudit logiciel. De telles informations sont susceptibles de

rendre inopérantes les tentatives de surveillance à l'aide des logiciels dont l'utilisation aurait été révélée. Le recourant ne parvient ainsi pas à démontrer qu'il n'y aurait plus de secret quant à l'acquisition de Pegasus par l'intimé.

Le Tribunal administratif fédéral n'a par conséquent pas violé le droit fédéral en retenant que les mesures de surveillance des autorités de poursuite pénale pourraient être entravées par une divulgation de l'information requise, de sorte que l'intérêt au maintien du secret pouvait se fonder sur l' art. 7 al. 1 let. b LTrans . Pour autant qu'il soit recevable, le grief doit être écarté.

E. 6.5.1

En application de l' art. 7 al. 1 let . c LTrans, le droit d'accès est limité, différé ou refusé lorsque l'accès à un document officiel risque de compromettre la sûreté intérieure ou extérieure de la Suisse.

Selon le Message relatif à la LTrans, cette exception vise essentiellement les activités policières, douanières, de renseignements et militaires. Elle permet 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 ou à mettre en danger les personnes si elles étaient rendues accessibles (FF 2003 1851 ch. 2.2.2.1.3).

Un risque de mise en péril de la sûreté intérieure ou extérieure est admis lorsque la divulgation d'un document ou d'une information emporterait un risque élevé d'attaque (STEIMEN, op. cit., no 22 ad art. 7 LTrans). Les informations touchant l'organisation, l'activité et la stratégie d'autorités compétentes notamment en matière de sûreté ou encore les logiciels spéciaux de surveillance utilisés par ces autorités peuvent aussi être concernés par l'exception de l' art. 7 al. 1 let . c LTrans (STEIMEN, op. cit., no 22 ad art. 7 LTrans ; voir à ce sujet l'arrêt du TAF A-700/2015 du 26 mai 2015, consid. 6 ss, concernant une demande d'accès adressée au Service Surveillance de la correspondance par poste et télécommunication [SCPT] et visant l'accès à une liste des noms et des numéros de version de tous les logiciels utilisés par le Service SCPT dans l'accomplissement de ses tâches).

E. 6.5.2

En l'espèce, le TAF a retenu que l'accès aux informations et aux éventuels documents demandés représenterait aussi une menace sérieuse pour la sécurité intérieure, de sorte que le maintien du secret se justifiait aussi à ce titre.

Il a considéré qu'il existait 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 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: 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 créées - pouvait être utilisé à des fins malveillantes par des tiers, les autorités de poursuite pénale et le SRC seraient privés d'un instrument efficace et essentiel dans la lutte contre la criminalité, dans la détection précoce et la prévention de menaces pour la sécurité de la Suisse. L'instance précédente en a déduit que le maintien du secret se justifiait aussi en raison de la menace qu'une divulgation représenterait pour la sécurité intérieure de la Suisse

(art. 7 al. 1 let . c LTrans).

E. 6.5.3

Pour critiquer ce raisonnement, le recourant se borne à exposer que le TAF se serait contenté de redites relatives à l'argumentation développée en lien avec l'exception de l' art. 7 al. 1 let. b LTrans . Il affirme péremptoirement que "tous les criminels du calibre de ceux poursuivis par fedpol sont nantis des capacités de Pegasus depuis à tout le moins l'été 2021 et ils se sont adaptés". Il avance encore que l'utilisation du logiciel en tant qu'il comporte une

backdoor compromettrait la sécurité de la Suisse et constituerait une véritable menace. Le recourant mentionne ainsi pêle-mêle des éléments de fait ne ressortant pas de l'arrêt attaqué. Sa critique est donc irrecevable sur ces points.

Le recourant défend en réalité l'intérêt public à garantir une utilisation des

GovWare conforme aux droits fondamentaux des personnes surveillées. En effet, il existe un intérêt public important à la transparence, qui consiste en particulier à savoir si le logiciel Pegasus est à disposition des autorités suisses ou non, compte tenu des révélations au sujet de ce logiciel et de l'entreprise l'ayant développé. Il résulte en effet des enquêtes menées à la suite des révélations concernant Pegasus que ce programme, mais aussi d'autres logiciels similaires, ont été utilisés comme outils de piratage et de surveillance visant des journalistes, des avocats, des responsables politiques et des militants des droits humains dans plusieurs États membres du Conseil de l'Europe et dans d'autres pays encore (cf. 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'État" du 20 septembre 2023 [Doc. 15825]). Le scandale qui s'est répandu dans l'opinion publique entourant l'utilisation de logiciels espions par les États dépasse ainsi le seul logiciel Pegasus et donc l'objet de la présente procédure.

Cela étant, le recourant ne prétend pas que le cadre législatif suisse tel qu'institué par le CPP, ainsi que les mécanismes prévus d'autorisation judiciaire et de communication à la personne concernée à la fin de la surveillance (cf. art. 279 CPP ; voir

supra consid. 5) ne permettraient pas de s'assurer d'une utilisation licite et proportionnée des

GovWare par les autorités suisses en disposant. De plus, comme le relève le TAF, les ministères publics cantonaux et fédéral tiennent une statistique annuelle des surveillances au moyen d'un

GovWare , qui indique notamment le type d'infractions, et qui doit être transmise au Service SCPT, lequel publie chaque année une statistique consolidée (cf. art. 269ter 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.

E. 6.6

Le recourant reproche enfin sommairement au TAF d'avoir méconnu le principe de la proportionnalité en ne permettant pas un caviardage. Un éventuel caviardage tel que requis par le recourant en application du principe de proportionnalité n'a toutefois guère lieu d'être lorsqu'il s'agit - comme en l'espèce - de garder secrète une information sur l' (in) existence d'un document.

E. 7

Il s'ensuit que le recours en matière de droit public doit être rejeté dans la mesure de sa recevabilité.

Le recourant, qui succombe, doit supporter les frais de la présente procédure (art. 66 LTF). Il n'y a pas lieu d'allouer de dépens (art. 68 al. 3 LTF).