Untersuchungsorgan der Administrativuntersuchung *«Datenabfluss»*

Organe chargé de l'enquête administrative *«Fuite de données»*

Organo d'inchiesta amministrativa *«Fuga di dati»*

Enquête administrative *« Fuite de données »*

Rapport

28 mars 2024

A l'attention de l'Organe de coordination (SG-DFF)

TABLE DES MATIERES

TABLE DES ABRÉVIATIONS

Abréviation	Définition
aDITAF	Directives du Conseil fédéral concernant l'informatique et la télécommunication dans l'administration fédérale du 23 février 2000 (ce texte n'est plus en vigueur)
AFC	Administration fédérale des contributions
aLPD	Loi fédérale sur la protection des données du 19 juin 1992 (ce texte n'est plus en vigueur)
aOCSP	Ordonnance sur les contrôles de sécurité relatifs aux personnes du 4 mars 2011 (ce texte n'est plus en vigueur)
aOIAF	Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale du 9 décembre 2011 (ce texte n'est plus en vigueur)
aOPCy	Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale du 27 mai 2020 (ce texte n'est plus en vigueur)
aOPD	Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (ce texte n'est plus en vigueur)
aOPrI	Ordonnance concernant la protection des informations de la Confédération du 4 juillet 2007 (ce texte n'est plus en vigueur)
armasuisse	Office fédéral de l'armement
ATAF	Arrêt du Tribunal administratif fédéral
ATF	Arrêt du Tribunal fédéral
BAC	Base d'aide au commandement
BSE	*Betriebssicherheitserklärung*
CA	Conférence des achats de la Confédération
CC	Code civil suisse du 10 décembre 1907
CDF	Contrôle fédéral des finances
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales conclue à Rome le 4 novembre 1950
CEO	*Chief Executive Officer*
CG	Conditions générales de la Confédération
Cgfr	Corps des gardes-frontières
CI	Conseil de l'informatique de la Confédération
Cmdt Cyber	Commandement Cyber
Cmdt Op / Cmdt des Opérations	Commandement des Opérations
CO	Loi fédérale complétant le Code civil suisse du 30 mars 1911
Concept SIPD	Concept de sécurité de l'information et de protection des données
CP	Code pénal suisse du 21 décembre 1937
CSI-DFJP	Centre de services informatiques CSI-DFJP
CSN	Cyberstratégie nationale
CSP	Contrôle de sécurité relatif aux personnes
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999

DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
DSIO	Délégué à la sécurité informatique des unités administratives (en allemand : ISBO)
fedpol	Office fédéral de la police
FF	Feuille fédérale
FOSC	Feuille officielle suisse du commerce
GA	Gestion des affaires et des dossiers
IPAS	Système d'information de fedpol nommé « *Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem des Bundesamtes für Polizei* »
Janus	Système d'information de la PJF nommé « *Elektronisches Informationssystem der Bundeskriminalpolizei* »
JORASYS	Système de journal et de rapport de la Police militaire
LAAM	Loi fédérale sur l'armée et l'administration militaire du 3 février 1995
LAr	Loi fédérale sur l'archivage du 26 juin 1998
LMP	Loi fédérale sur les marchés publics du 21 juin 2019
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 21 mars 1997
LOGA	Loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997
LParl	Loi sur l'Assemblée fédérale du 13 décembre 2002
LPD	Loi fédérale sur la protection des données du 25 septembre 2020
LPers	Loi sur le personnel de la Confédération du 24 mars 2000
LRens	Loi fédérale sur le renseignement du 25 septembre 2015
LSI	Loi fédérale sur la sécurité de l'information du 18 décembre 2020
LSIA	Loi fédérale sur les systèmes d'information de l'armée et du DDPS du 3 octobre 2008
LSIP	Loi fédérale sur les systèmes d'information de police de la Confédération du 13 juin 2008
LTrans	Loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004
MOT	Mesures organisationnelles et techniques, connues également sous l'acronyme TOMs
MPC	Ministère public de la Confédération
NCSC	Centre national pour la cybersécurité
OA	OBERSON ABELS SA
OCSP	Ordonnance sur les contrôles de sécurité relatifs aux personnes du 8 novembre 2023

OFCL	Office fédéral des constructions et de la logistique
OFCS	Office fédéral de la cybersécurité
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OLOGA	Ordonnance sur l'organisation du gouvernement et de l'administration du 25 novembre 1998
OPDo	Ordonnance sur la protection des données du 31 août 2022
OPSEnt	Ordonnance sur la procédure de sécurité relative aux entreprises du 8 novembre 2023
Ordonnance GPDA	Ordonnance sur le système électronique de gestion de personnes, de dossiers et d'affaires de l'Office fédéral de la justice du 23 septembre 2016
Ordonnance IPAS	Ordonnance sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police du 15 octobre 2008
Ordonnance JANUS	Ordonnance sur le système informatisé de la Police judiciaire fédérale du 30 novembre 2001
Ordonnance PAGIRUS	Ordonnance sur le système de gestion de personnes, de dossiers et d'affaires (PAGIRUS) de l'Office fédéral de la justice du 16 décembre 2009
Ordonnance SNE	Ordonnance sur le Système national d'enquête du 15 octobre 2008
Ordonnance SYMIC	Ordonnance sur le système d'information central sur la migration du 12 avril 2006
Org-OMP	Ordonnance sur l'organisation des marchés publics de l'administration fédérale du 24 octobre 2012
OSI	Ordonnance sur la sécurité de l'information dans l'administration fédérale et l'armée du 8 novembre 2023
OSIAr	Ordonnance sur les systèmes d'information de l'armée et du DDPS du 16 décembre 2009
OTNI	Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale du 25 novembre 2020
OTUIC	Ordonnance sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération du 22 février 2012
PA	Loi fédérale sur la procédure administrative du 20 décembre 1968
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJF	Police judiciaire fédérale
PM	Police militaire
PPS	Unité « *Planung, Projektsteuerung und Standardisierung der Polizeilichen Informationsverarbeitung* » qui appartenait à la division des Ressources de fedpol jusqu'à fin 2008

PSE	Procédure de sécurité relative aux entreprises
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral
SEM	Secrétariat d'Etat aux migrations
SEPOS	Secrétariat d'Etat à la politique de sécurité
SNE	Système national d'enquête
SRC	Service de renseignement de la Confédération
SG	Secrétariat général
SG-DFF	Secrétariat général du Département fédéral des finances
TAF	Tribunal administratif fédéral
TIC	Technologies de l'information et de la communication
TOMs	*Technical and organisational measures*, connues également sous l'acronyme MOT (« mesures organisationnelles et techniques »)
Unités	Unités administratives ou organisationnelles de la Confédération
VASS	*Verwaltung von Asservaten, Spuren und Spurenträgern*
Xplain	Xplain SA
ZEMIS	*Zentrale Migrationsinformationssystem* (système d'information central sur la migration SYMIC)

I. RÉSUMÉ

FR

L'enquête administrative *« Fuite de données »* s'est déroulée entre le 1er septembre 2023 et le 28 mars 2024.

A la suite de la publication sur le darknet en juin 2023 de données dérobées à l'entreprise Xplain SA (ci-après « Xplain »), qui comprenaient des données de la Confédération, le Conseil fédéral a ordonné le 23 août 2023 l'ouverture d'une enquête administrative. L'enquête s'étendait à tous les départements et à la Chancellerie fédérale.

Notre étude OBERSON ABELS SA a été désignée comme organe chargé de l'enquête.

L'enquête visait d'abord à déterminer les circonstances, du côté de l'administration fédérale, qui ont permis à Xplain d'entrer en possession de données productives de ladite administration[1].

L'organe chargé de l'enquête devait ensuite déterminer (i) si des déficiences en matière technique, d'organisation ou de processus ont conduit à ce que des données productives de l'administration fédérale soient en possession de Xplain et (ii) si l'administration fédérale a satisfait à ses devoirs de manière adéquate lors du choix, de l'instruction et de la surveillance de Xplain ainsi que dans le cadre de la collaboration avec celle-ci.

Enfin, l'organe chargé de l'enquête devait évaluer de manière approfondie les problèmes identifiés indépendamment du cas Xplain et élaborer des solutions et des recommandations visant à réduire les risques pour la sécurité. Il n'était toutefois pas attendu que l'organe d'enquête procède à un examen technique de l'informatique.

Au terme de l'enquête, nous parvenons aux **conclusions suivantes**.

Un département et 11 unités administratives de trois autres départements[2] sont **touchés par l'enquête** :

Département fédéral des affaires étrangères (DFAE) ;

Commandement des Opérations (cdmt Op), auquel appartient la Police militaire (PM),

Office fédéral de l'armement (armasuisse) ;

Base d'aide au commandement (BAC) ;

Centre de services informatiques CSI-DFJP (CSI-DFJP) ;

Office fédéral de la police (fedpol) ;

Office fédéral des constructions et de la logistique (OFCL) ;

Office fédéral de la douane et de la sécurité des frontières (OFDF) ;

Office fédéral de l'informatique et de la télécommunication (OFIT) ;

Office fédéral de la justice (OFJ) ;

Secrétariat d'Etat aux migrations (SEM) ;

Service de renseignement de la Confédération (SRC).

[1] Nous avons défini dans ce rapport les « données productives » de la Confédération comme suit : « données réelles issues des systèmes d'information de la Confédération, par opposition aux données tests ou anonymisées ».
[2] DFJP, DFF, DDPS.

Parmi les Unités touchées par l'enquête, les unités suivantes (« Unités directement concernées ») utilisaient dans l'environnement informatique de la Confédération des produits développés par Xplain dans lesquels leurs données étaient traitées : fedpol, OFDF, OFJ, PM et SEM.

Les circonstances factuelles qui ont **conduit** à ce que des données productives de certaines unités de la Confédération soient présentes dans l'environnement informatique de Xplain peuvent être résumées comme suit :

> Premièrement, des employés de Xplain ont envoyé, depuis le compte e-mail de la Confédération mis à leur disposition dans le cadre de la collaboration entre Xplain et une Unité directement concernée, vers leur compte e-mail auprès de Xplain ou vers le compte e-mail de leurs collègues auprès de Xplain, des données productives reçues d'employés de la Confédération. Dans un cas à tout le moins, un employé de Xplain a selon toute vraisemblance extrait lui-même des données d'un système de production de fedpol et ces données se sont ensuite trouvées dans l'environnement informatique de Xplain.
>
> Deuxièmement, des employés de la Confédération en charge du support informatique interne ont traité des demandes d'utilisateurs contenant des données productives et les ont transmises à Xplain ou les ont mises à disposition de Xplain sur un serveur partagé, sans préalablement retirer, pseudonymiser ou caviarder les données productives.
>
> Troisièmement, des employés de la Confédération participant à des travaux de développement, de test ou de migration informatique, ont transmis à Xplain des données productives dans le cadre de ces travaux.

Nous ne pouvons pas définitivement exclure l'existence d'autres canaux ayant conduit à la présence de données productives de la Confédération dans l'environnement informatique de Xplain. Par ailleurs, l'enquête a permis d'identifier des situations dans lesquelles des données productives de la Confédération sont parvenues dans l'environnement informatique de Xplain, sans que ces données ne se trouvent sur le darknet en juin 2023.

Les cas de transmission de données productives à Xplain apparaissent **isolés**, d'une part, à l'échelle de la correspondance entre Xplain et les Unités touchées par l'enquête et, d'autre part, à l'échelle de la correspondance entre Xplain et chaque employé de la Confédération ou chaque employé de Xplain ayant transmis à une occasion au moins des données productives à Xplain.

Toutefois, comme l'illustrent les cas examinés dans ce rapport, en matière de sécurité de l'information et de protection des données, **un seul transfert à un tiers suffit potentiellement** :

- Pour que la sécurité de l'information et la protection des données soient compromises.
- Pour que des volumes importants de données soient en mains d'un tiers.
- Pour que des données sensibles ou classifiées soient en mains d'un tiers.

Les principales **déficiences** mises en évidence par l'enquête administrative sont les suivantes.

> Premièrement, une déficience en termes de **processus** : des employés de la Confédération et des employés d'un fournisseur externe, Xplain, ont pu extraire des données de systèmes de production de la Confédération et envoyer ces données par e-mail à Xplain sans qu'un processus n'encadre apparemment ces démarches et, en particulier, sans que le principe des quatre yeux ne soit respecté à chaque étape.

Deuxièmement, une déficience en termes de **technique** : aucune mesure technique n'est venue faire obstacle aux extractions de données productives précitées, ni à l'envoi par e-mail de données productives vers un fournisseur externe.

Troisièmement, les cas décrits dans ce rapport mettent en lumière un déficit en termes de **formation et de sensibilisation** des personnes appelées à traiter des données des systèmes en question au sein de la Confédération. En outre, après qu'une unité a identifié une fonctionnalité conduisant potentiellement à des flux de données productives dans le cadre de demandes de support, l'information n'apparaît pas avoir circulé entre les Unités directement concernées.

Sous l'angle de la **sécurité de l'information**, nous parvenons à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération a partiellement rempli ses devoirs de choisir avec soin et d'instruire adéquatement. En revanche, le devoir de surveiller n'a pas été rempli dans ce contexte.

Sous l'angle de la **protection des données personnelles**, nous parvenons à la conclusion que, dans les cas de sous-traitance à Xplain qui ont été identifiés, la Confédération n'a pas rempli ses devoirs de choisir avec soin, d'instruire adéquatement et de surveiller.

Les cas de transmission de données productives à Xplain et les violations retenues par l'organe d'enquête, du côté de la Confédération, aux devoirs de choisir avec soin, instruire adéquatement et surveiller sont intervenus dans un **contexte** qui les a favorisés, mais non causés :

Sous l'angle de la gestion des cybermenaces des tiers, les Unités touchées par l'enquête paraissent avoir **sous-estimé**, pour certaines jusqu'à la fuite de données de juin 2023, les risques posés par des tiers, notamment les fournisseurs de logiciels.

L'enquête révèle des compréhensions parfois divergentes de la **répartition des responsabilités** en matière de sécurité de l'information entre, suivant les situations, (i) le service d'achat central, (ii) le service demandeur, (iii) le département auquel le service demandeur appartient, (iv) le CSI-DFJP, (v) l'OFIT, (vi) voire entre certains collaborateurs d'un même service.

Un consensus se dégage des interrogatoires selon lequel les ressources allouées à la sécurité de l'information au sein des Unités directement concernées étaient globalement **insuffisantes**.

L'enquête révèle une situation de **dépendance** des Unités directement concernées à l'égard de Xplain au cours des années sous enquête.

La relation entre Xplain et les Unités directement concernées semblent avoir reposé essentiellement sur la **confiance**.

Les enseignements tirés de la présente enquête administrative appellent à notre sens des recommandations tant sur le plan organisationnel, que sur le fond. Ces **recommandations** sont exposées au chapitre VI.B.

DE

Die Administrativuntersuchung «Datenabfluss» fand zwischen dem 1. September 2023 und dem 28. März 2024 statt.

Nachdem im Juni 2023 im Darknet Daten veröffentlicht worden waren, die der Firma Xplain AG («Xplain») entwendet worden waren und die auch Daten des Bundes enthielten, ordnete der Bundesrat am 23. August 2023 die Eröffnung einer Administrativuntersuchung an. Die Untersuchung erstreckte sich auf alle Departemente und die Bundeskanzlei.

Unsere Kanzlei OBERSON ABELS SA wurde als Untersuchungsorgan beauftragt.

Die Administrativuntersuchung sollte zunächst aufzeigen, welche Umstände es auf Seiten der Bundesverwaltung ermöglicht haben, dass Xplain in den Besitz von produktiven Daten der Bundesverwaltung kam[3].

Das Untersuchungsorgan hatte ferner zu klären, (i) ob technische, organisatorische oder prozesshafte Mängel dazu geführt haben, dass Produktivdaten der Bundesverwaltung im Besitz von Xplain waren und (ii) ob die Bundesverwaltung bei der Auswahl, Instruktion und Überwachung der Xplain sowie bei der Zusammenarbeit mit dieser Firma die Pflichten angemessen erfüllt hat.

Schliesslich sollte das Untersuchungsorgan die unabhängig vom Fall Xplain erkannten Probleme vertieft beurteilen sowie Lösungsansätze und Empfehlungen zur Reduktion der Sicherheitsrisiken erarbeiten. Es wurde jedoch nicht erwartet, dass das Untersuchungsorgan eine technische Informatikprüfung durchführt.

Nach Abschluss der Untersuchung kommen wir zu den folgenden Schlussfolgerungen.

Ein Departement und 11 Verwaltungseinheiten aus drei weiteren Departementen[4] sind von der Untersuchung betroffen:

Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)

Kommando Operationen (Kdo Op), dem die Militärpolizei (MP) angehört

Bundesamt für Rüstung (armasuisse)

Führungsunterstützungsbasis (FUB)

Informatik Service Center ISC-EJPD

Bundesamt für Polizei (fedpol)

Bundesamt für Bauten und Logistik (BBL)

Bundesamt für Zoll und Grenzsicherheit (BAZG)

Bundesamt für Informatik und Telekommunikation (BIT)

Bundesamt für Justiz (BJ)

Staatssekretariat für Migration (SEM)

Nachrichtendienst des Bundes (NDB)

[3] Wir haben in diesem Bericht die «produktiven Daten» der Bundesverwaltung wie folgt definiert: «tatsächliche Daten aus den Informationssystemen des Bundes, im Gegensatz zu Testdaten oder anonymisierten Daten».
[4] EJPD, EFD, VBS.

Von den von der Untersuchung betroffenen Einheiten nutzten die folgenden Einheiten («Direkt betroffene Einheiten») in der IT-Umgebung des Bundes von Xplain AG entwickelte Produkte, in denen ihre Daten verarbeitet wurden: fedpol, BAZG, BJ, MP und SEM.

Die tatsächlichen Umstände, die dazu **führten**, dass Produktivdaten von bestimmten Verwaltungseinheiten in der IT-Umgebung von Xplain vorhanden waren, lassen sich wie folgt zusammenfassen:

> Erstens haben Mitarbeiter von Xplain vom E-Mail-Konto des Bundes, das ihnen im Rahmen der Zusammenarbeit zwischen Xplain und einer direkt betroffenen Einheit zur Verfügung gestellt wurde, an ihr E-Mail-Konto bei Xplain oder an das E-Mail-Konto ihrer Kollegen bei Xplain produktive Daten versendet, die sie von Mitarbeitern des Bundes erhalten haben. Zumindest in einem Fall hat ein Mitarbeiter von Xplain aller Wahrscheinlichkeit nach selbst Daten aus einem Produktionssystem von fedpol extrahiert, und diese Daten sind dann in die IT-Umgebung von Xplain gelangt.
>
> Zweitens bearbeiteten Mitarbeiter vom Bund, die für den internen IT-Support zuständig waren, Nutzeranfragen, die Produktivdaten enthielten, und leiteten sie an Xplain weiter oder stellten sie Xplain auf einem gemeinsam genutzten Server zur Verfügung, ohne die Produktivdaten zuvor zu entfernen, zu pseudonymisieren oder zu schwärzen.
>
> Drittens: Mitarbeiter des Bundes, die an IT-Entwicklungs-, Test- oder Migrationsarbeiten beteiligt waren, übermittelten Xplain im Rahmen dieser Arbeiten Produktivdaten.

Wir können nicht endgültig ausschliessen, dass es andere Kanäle gab, die dazu geführt haben, dass Produktivdaten des Bundes in der IT-Umgebung von Xplain vorhanden waren. Darüber hinaus wurden im Rahmen der Untersuchung Situationen identifiziert, in denen Produktivdaten des Bundes in die IT-Umgebung von Xplain gelangt sind, ohne dass sich diese Daten im Juni 2023 im Darknet befanden.

Die Fälle, in denen Produktivdaten an Xplain übermittelt wurden, erscheinen **isoliert**, einerseits auf der Ebene der Korrespondenz zwischen Xplain und den von der Untersuchung betroffenen Verwaltungseinheiten, und andererseits auf der Ebene der Korrespondenz zwischen Xplain und jedem Mitarbeiter des Bundes oder jedem Mitarbeiter von Xplain, der mindestens einmal Produktivdaten an Xplain übermittelt hat.

Wie die in diesem Bericht untersuchten Fälle zeigen, reicht in Bezug auf Informationssicherheit und Datenschutz jedoch potenziell **eine einzige Weitergabe an einen Dritten** aus:

- Um die Informationssicherheit und den Datenschutz zu gefährden.
- Damit grosse Datenmengen in die Hände eines Dritten gelangen.
- Damit besonders schützenswerte oder klassifizierte Daten in die Hände eines Dritten gelangen.

Im Folgenden werden die wichtigsten **Mängel** aufgeführt, die im Rahmen der Administrativuntersuchung festgestellt wurden.

> Erstens, ein **Prozessmangel**: Angestellte des Bundes und Angestellte eines externen Lieferanten, Xplain, konnten Daten aus Produktionssystemen des Bundes extrahieren und per E-Mail an Xplain senden, ohne dass es offensichtlich einen Prozess für diese Schritte gab und insbesondere ohne, dass das Vier-Augen-Prinzip bei jedem Schritt beachtet wurde.
>
> Zweitens, ein Mangel in **technischer Hinsicht**: Es gab keine technischen Massnahmen, die die oben genannten Extraktionen von Produktivdaten oder das Versenden von Produktivdaten per E-Mail an einen externen Anbieter behinderten.

Drittens zeigen die in diesem Bericht beschriebenen Fälle ein Defizit in Bezug auf die **Ausbildung und Sensibilisierung** der Personen auf, die innerhalb des Bundes Daten aus den fraglichen Systemen bearbeiten. Nachdem eine Einheit eine Funktionalität identifiziert hat, die potenziell zu produktiven Datenflüssen im Rahmen von Support-Anfragen führt, scheint die Information ausserdem nicht zwischen den direkt betroffenen Einheiten geflossen zu sein.

Aus Sicht der **Informationssicherheit** kommen wir zum Schluss, dass der Bund in den Beziehungen der direkt betroffenen Einheiten zu Xplain vor dem Datenabfluss im Juni 2023 seine Pflichten, sorgfältig auszuwählen und angemessen zu instruieren, teilweise erfüllt hat. Die Überwachungspflicht wurde in diesem Zusammenhang hingegen nicht erfüllt.

Aus Sicht des **Datenschutzes** kommen wir zum Schluss, dass der Bund in den identifizierten Fällen der Bearbeitung von Personendaten durch Xplain als Auftragsbearbeiter seine Pflichten zur sorgfältigen Auswahl, zur angemessenen Instruktion und zur Überwachung nicht erfüllt hat.

Die Fälle der Weitergabe von Produktivdaten an Xplain und die vom Untersuchungsorgan festgestellten Verstösse gegen die Pflichten zur sorgfältigen Auswahl, angemessenen Anleitung und Überwachung auf Seiten des Bundes fanden in einem **Kontext** statt, der sie begünstigte, aber nicht verursachte:

Unter dem Aspekt des Umgangs mit Cyberbedrohungen durch Dritte scheinen die von der Untersuchung betroffenen Einheiten die von Dritten, insbesondere von Softwareanbietern, ausgehenden Risiken **unterschätzt** zu haben, einige von ihnen sogar bis zum Datenabfluss im Juni 2023.

Die Untersuchung zeigt ein teilweise unterschiedliches Verständnis der **Verteilung der Verantwortung** für die Informationssicherheit zwischen, je nach Situation, (i) der zentralen Beschaffungsstelle, (ii) der Bedarfsstelle, (iii) dem Departement, dem die Bedarfsstelle angehört, (iv) dem ISC-EJPD, (v) dem BIT, (vi) oder sogar zwischen einzelnen Mitarbeitenden derselben Stelle.

Aus den Befragungen ergab sich ein Konsens, dass die Ressourcen, die in den direkt betroffenen Einheiten für die Informationssicherheit bereitgestellt wurden, insgesamt **unzureichend** waren.

Die Untersuchung zeigt, dass die direkt betroffenen Einheiten in den untersuchten Jahren von Xplain **abhängig** waren.

Die Beziehung zwischen Xplain und den direkt betroffenen Einheiten scheint im Wesentlichen auf **Vertrauen** beruht zu haben.

Die aus der vorliegenden Administrativuntersuchung gezogenen Lehren erfordern unserer Ansicht nach Empfehlungen sowohl in organisatorischer als auch in inhaltlicher Hinsicht. Diese **Empfehlungen** werden in Kapitel VI.B. erläutert.

II. OBJET DE L'ENQUÊTE

1 L'objet de l'enquête a été défini comme suit par le Conseil fédéral le 23 août 2023 :

> *« Die Administrativuntersuchung soll insbesondere aufzeigen, welche Umstände es auf Seiten der Bundesverwaltung ermöglicht haben, dass Xplain AG in den Besitz von produktiven Daten der Bundesverwaltung kam und ob bei der Auswahl, Instruktion und Überwachung der Xplain AG sowie bei der Zusammenarbeit mit dieser Firma die Pflichten angemessen erfüllt wurden. Ferner ist zu prüfen, welche Prozesse und Vorgaben in der Bundesverwaltung anzupassen sind, um künftig die Sicherheitsrisiken, die mit der Übermittlung von Informationen der Bundesverwaltung, darunter klassifizierten Informationen und Personendaten, an externe Dienstleister sowie mit deren Bearbeitung verbunden sind, besser erkennen, adressieren und mitigieren zu können.*
>
> *Die Administrativuntersuchung erstreckt sich auf alle Departemente und die Bundeskanzlei; sie richtet sich nicht gegen bestimmte Personen.*
>
> *Die Untersuchung ist in maximal zwei Etappen durchzuführen. In der ersten Etappe ist retrospektiv der Sachverhalt im Fall Xplain AG zu klären und es sind allfällige Sofortmassnahmen vorzuschlagen. Soweit nötig, sind in der zweiten Etappe unabhängig vom Fall Xplain AG erkannte Probleme vertieft zu beurteilen sowie Lösungsansätze und Empfehlungen zur Reduktion der Sicherheitsrisiken zu erarbeiten. »*
>
> Soit en traduction libre :
>
> *« L'enquête administrative doit notamment montrer quelles circonstances, du côté de l'administration fédérale, ont permis à Xplain SA d'entrer en possession de données productives de l'administration fédérale et si les devoirs ont été remplies de manière adéquate lors du choix, de l'instruction et de la surveillance de Xplain SA ainsi que lors de la collaboration avec cette entreprise. Il convient en outre d'examiner quels processus et quelles prescriptions doivent être adaptés au sein de l'administration fédérale afin de mieux identifier, traiter et limiter à l'avenir les risques de sécurité liés à la transmission à des prestataires de services externes, et au traitement, d'informations de l'administration fédérale, dont les informations classifiées et des données personnelles.*
>
> *L'enquête administrative s'étend à tous les départements et à la Chancellerie fédérale ; elle n'est pas dirigée contre des personnes spécifiques.*
>
> *L'enquête doit être menée en deux étapes au maximum. Lors de la première étape, il s'agira de clarifier rétrospectivement les faits dans le cas Xplain SA et de proposer d'éventuelles mesures immédiates. Si nécessaire, la deuxième étape consistera à évaluer de manière approfondie les problèmes identifiés indépendamment du cas Xplain SA et à élaborer des solutions et des recommandations visant à réduire les risques pour la sécurité. »*

2 Le calendrier de l'enquête a été défini comme suit par le Conseil fédéral : *« Die Untersuchung soll am 1. September 2023 starten und ist spätestens am 31. März 2024 abzuschliessen. »,* soit en traduction libre *« L'enquête doit débuter le 1er septembre 2023 et s'achever au plus tard le 31 mars 2024.* »

3 Le Conseil fédéral a en outre désigné le Département fédéral des finances (DFF) comme organe de coordination pour la préparation et le suivi de l'enquête administrative (ci-après « **l'Organe de coordination** »). L'organe de coordination a réuni un groupe de travail (« *Kerngruppe* »), qui l'assiste dans ses tâches. Ce groupe est composé de représentants du (i) Secrétariat général (SG) du DFF (le « **SG-DFF** »),

(ii) du SG du Département fédéral de la défense, de la protection de la population et des sports (« **DDPS** »), (iii) du SG du Département fédéral de justice et police (« **DFJP** »), de la Chancellerie fédérale, (iv) de Office fédéral de l'armement (« **armasuisse** »), (v) de l'Office fédéral des constructions et de la logistique (« **OFCL** »), (vi) du Centre national pour la cybersécurité (« **NCSC** ») et (vii) de l'Office fédéral de l'informatique et de la télécommunication (« **OFIT** ») (le « **Groupe de travail** »).

4 Le 24 août 2023, un contrat de mandat a été conclu en ce sens entre la Confédération suisse, agissant par le SG-DFF, et OBERSON ABELS SA. Ce contrat prévoit en particulier, sous son art. 1.2, ce qui suit :

> *« Die Administrativuntersuchung soll in maximal zwei Etappen durchgeführt werden. Die Etappierung erfolgt vor dem Hintergrund, dass rasch erste Lehren aus dem Vorfall Xplain AG gezogen werden können sollen (1. Etappe). Die erste Etappe soll retrospektiv untersuchen, unter welchen Umständen die Xplain AG von den Verwaltungseinheiten beauftragt worden war und ob auf Seiten der Bundesverwaltung bei der Auswahl, Instruktion und Überwachung der Xplain AG sowie bei der Zusammenarbeit mit Xplain AG Pflichten verletzt wurden (Offertanfrage Ziff. 2.2.1 Absatz 1).*
>
> *Ferner ist zu klären, ob technische, prozesshafte oder organisatorische Mängel dazu geführt haben, dass Produktivdaten der Bundesverwaltung im Besitz der Xplain AG waren und ob dabei die Sicherheitsrisiken falsch eingeschätzt oder übersehen wurden. Es ist aufzuzeigen, welche Sofortmassnahmen zu ergreifen sind, um Sicherheitsrisiken zu beheben. Zur ersten Etappe soll ein Bericht erstellt werden. Dieser soll die Erkenntnisse aus der ersten Etappe und Empfehlungen zum weiteren Vorgehen enthalten (Offertanfrage Ziff. 2.2.1 Absatz 2). Es wird jedoch nicht erwartet, dass die Anbieterin eine technische Informatikprüfung durchführt.*
>
> *Je nach Erkenntnissen in diesem Bericht wird die Administrativuntersuchung fortgeführt oder nicht. Die zweite Etappe ist als Option ausgestaltet (Offertanfrage Ziff. 2.2.1 Absatz 3).*
>
> *In einer allfälligen zweiten Etappe soll anhand der Befunde der ersten Etappe geprüft werden, welche Massnahmen unabhängig vom Fall Xplain AG zu treffen sind, um künftig die Sicherheitsrisiken, die mit der Leistungserbringung bzw. mit dem Informationszugriff durch externe Dienstleister verbunden sind, besser erkennen, adressieren und mitigieren zu können. Zum Abschluss der allfälligen zweiten Etappe bzw. zum Abschluss der Administrativuntersuchung soll ein Schlussbericht gemäss Art. 27j Abs. 1 und 2 RVOV mit Ergebnissen und Empfehlungen erstellt werden (vgl. Offertanfrage Ziff. 2.2.1 Absatz 4).»*
>
> Soit en traduction libre :
>
> *« L'enquête administrative doit être menée en deux étapes au maximum. L'objectif de la division en étapes est de pouvoir tirer rapidement les premiers enseignements de l'affaire Xplain SA (1^e^ étape). La première étape doit examiner rétrospectivement dans quelles circonstances Xplain SA a été mandatée par les unités administratives et si l'administration fédérale a manqué à ses devoirs lors du choix, de l'instruction et de la surveillance ainsi que lors de la collaboration avec Xplain SA (demande d'offres, ch. 2.2.1, al. 1).*
>
> *Il convient en outre de déterminer si des déficiences en matière technique, d'organisation ou de processus ont conduit à ce que des données productives de l'administration fédérale soient en possession de Xplain SA et si les risques de sécurité ont été mal évalués ou négligés. Il convient de montrer quelles mesures immédiates doivent être prises pour éliminer les risques de sécurité. La première étape doit faire l'objet d'un rapport. Celui-ci doit contenir*

les conclusions de la première étape et des recommandations pour la suite des opérations (demande d'offres, ch. 2.2.1, al. 2). Il n'est toutefois pas attendu que l'organe d'enquête procède à un examen technique de l'informatique.

Selon les conclusions de ce rapport, l'enquête administrative sera poursuivie ou non. La deuxième étape est conçue comme une option (demande d'offres, ch. 2.2.1, al. 3).

Dans une éventuelle deuxième étape, il s'agira d'examiner, sur la base des résultats de la première étape, quelles mesures doivent être prises indépendamment du cas Xplain SA afin de mieux identifier, traiter et limiter à l'avenir les risques de sécurité liés à la fourniture de prestations ou à l'accès aux informations par des prestataires de services externes. A la fin de l'éventuelle deuxième étape, respectivement à la fin de l'enquête administrative, un rapport final doit être établi conformément à l'art. 27j, al. 1 et 2, OLOGA, avec les résultats et les recommandations (cf. demande d'offres, ch. 2.2.1, al. 4) »

5 Compte tenu de développements inattendus (mise à disposition de données plus complexe que prévue et nécessité pour le SG-DFF de disposer plus tôt de premiers résultats de l'enquête), un avenant au contrat a été signé le 7 décembre 2023. Cet avenant prévoit en particulier la fusion des deux étapes précitées :

« Neu wird die Etappierung der Untersuchungsteile und die optionale Ausgestaltung der zweiten Etappe aufgehoben. Die Anbieterin untersucht ab 22. November 2023 die oben beschriebenen retrospektiven und prospektiven Aspekte parallel und wird über beide gleichzeitig berichten. Der Gegenstand der Untersuchung bleibt aber insgesamt unverändert, wird also nicht auf weitere Lieferanten des Bundes oder Vorfälle ausgedehnt.»

Soit en traduction libre :

« La division de l'enquête en étapes et le caractère optionnel de la deuxième étape sont désormais supprimés. A partir du 22 novembre 2023, l'organe d'enquête examinera en parallèle les aspects rétrospectifs et prospectifs décrits ci-dessus et rendra compte des deux en même temps. L'objet de l'enquête reste toutefois globalement inchangé et ne sera donc pas étendu à d'autres fournisseurs de la Confédération ou à d'autres incidents. »

6 Conformément au mandat[5], ce rapport n'examine pas les faits sous l'angle du droit pénal.

III. DEROULEMENT DE L'ENQUÊTE

A. Etapes-clés

7 L'enquête administrative « *Fuite de données* » a débuté le 1er septembre 2023. Les principales étapes de l'enquête sont décrites dans les paragraphes qui suivent.

8 L'enquête administrative a été menée par une équipe au sein de OBERSON ABELS SA. Chaque membre de l'équipe a reçu, après examen des données recueillies, une déclaration de sécurité relative aux personnes[6]. L'expression « **Organe d'enquête** » ou l'abréviation « **OA** » utilisées dans ce rapport désignent cette équipe et non l'étude dans son ensemble.

[5] Voir ch. 2.2.2 de la demande d'offres, auquel renvoie le contrat de mandat (AUD B01.01.04.87).
[6] Cf. aOCSP du 4 mars 2011.

9 Le 4 septembre 2023, OA a adressé huit demandes de renseignements : une à la Chancellerie fédérale et une à chaque secrétariat général des sept Départements de l'administration fédérale[7]. Chaque demande visait pour l'essentiel les éléments suivants[8] :

- Liste exhaustive des unité(s) administrative(s) au sein du Département/de la Chancellerie fédérale qui ont, ou ont eu par le passé, des relations d'affaires avec Xplain AG (« **Xplain** ») ;
- Copie de tous les contrats conclus avec Xplain, y compris, notamment, lorsqu'une unité tierce a été mandatée par une unité administrative pour conclure un contrat pour le compte de cette dernière ;
- Identité des personnes au sein du Département/de la Chancellerie fédérale et ses unités administratives qui sont intervenues dans les relations d'affaires précitées avec Xplain ;
- Toutes directives, circulaires et autres instructions internes au Département/à la Chancellerie fédérale et ses unités administratives relatives à a) la gestion (y compris protection) des données (y compris données personnelles) et b) la cybersécurité.

10 Le 26 septembre 2023, l'Administration fédérale des contributions (« **AFC** ») a donné accès à OA à la plateforme forensique *Nuix Investigate* sur laquelle se trouvait une copie du « *Datendump* », soit le lot de données mises en ligne par le groupe de hackers « Play » en juin 2023, que le NCSC a téléchargé et trié[9].

11 Le 29 septembre 2023, sur la base des informations reçues de la Chancellerie fédérale et des Secrétariats généraux des Départements en réponse à ses demandes du 4 septembre 2023, OA a adressé 11 demandes de renseignements complémentaires aux unités de l'administration fédérale suivantes: Département fédéral des affaires étrangères (« **DFAE** »)[10] ; armasuisse[11] ; Base d'aide au commandement (« **BAC** »)[12] ; Centre de services informatiques CSI-DFJP (« **CSI-DFJP** »)[13] ; Office fédéral de la police (« **fedpol** »)[14] ; OFCL[15] ; Office fédéral de la douane et de la sécurité des frontières (« **OFDF** »)[16] ; OFIT[17] ; Office fédéral de la justice (« **OFJ** »)[18] ; Secrétariat d'Etat aux migrations (« **SEM** »)[19] ; Service de renseignement de la Confédération (« **SRC** »)[20]. Dans ce contexte, les 11 demandes susvisées requerraient essentiellement des unités en question les informations suivantes (hormis la demande envoyée au DFAE, qui ne comprenait que le ch. ii vu la réponse reçue à la demande du 4 septembre 2023) : i) liste des personnes exerçant actuellement, ou ayant exercé par le passé, une fonction dans certains secteurs au sein de l'unité concernée (Direction ; Juridique ; Achats ; Informatique) ; ii) liste des

[7] AUD 03.01.1-5 ; AUD 03.02.1-5 ; AUD 03.03.1-5 ; AUD 03.04.1-5 ; AUD 03.05.2-6 ; AUD 03.06.1-5 ; AUD 03.07.1-5 ; AUD 03.08.1-5.
[8] AUD 03.01.1-5 ; AUD 03.02.1-5 ; AUD 03.03.1-5 ; AUD 03.04.1-5 ; AUD 03.05.2-6 ; AUD 03.06.1-5 ; AUD 03.07.1-5 ; AUD 03.08.1-5.
[9] A ce sujet : NCSC, Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain, 14.12.2023, p. 5 s. Un total de 1'295'862 objets a été mis à notre disposition, ce qui correspond à l'intégralité des données publiées sur le Darknet selon le rapport précité.
[10] AUD 03.02.25-28.
[11] AUD 03.05.01.1-4.
[12] AUD 03.05.02.1-4.
[13] AUD 03.04.02.1-4.
[14] AUD 03.04.01.1-4.
[15] AUD 03.06.03.1-4.
[16] AUD 03.06.01.1-4.
[17] AUD 03.06.02.1-4.
[18] AUD 03.04.04.1-4.
[19] AUD 03.04.03.1-4.
[20] AUD 03.05.03.1-4.

organes, employés[21] ou mandataires de Xplain disposant actuellement, ou ayant disposé par le passé notamment d'un compte de messagerie de l'unité en question.

12 Ces unités (administratives ou organisationnelles) sont désignées ci-après collectivement comme les « Unités touchées par l'enquête ».

13 Vu les informations complémentaires fournies à OA lors d'une séance à Berne le 10 octobre 2023 avec l'Organe de coordination et le Groupe de travail, OA a envoyé une demande de renseignements à la Police militaire le 12 octobre 2023. Cette demande a un contenu analogue à celui des demandes précitées du 29 septembre 2023.

14 Le 20 octobre 2023, OA a envoyé trois demandes de mise à disposition de données aux prestataires internes de services informatiques concernés, à savoir à l'OFIT[22], à la BAC[23] et à la division informatique DFAE[24]. Ces demandes se fondaient sur les informations remises suite aux demandes de OA des 4 et 29 septembre 2023 et portaient sur un total de 421 comptes de messagerie professionnelle (comptes Exchange)[25].

15 Le 2 novembre 2023, OA a envoyé trois demandes complémentaires, analogues à celles du 20 octobre 2023 précitées, de mise à disposition de données aux prestataires internes de services informatiques concernés (l'OFIT, la BAC respectivement la division informatique DFAE) ; un total de 11 comptes Exchange était visé[26].

16 Le 10 novembre 2023, OA a demandé à fedpol[27] et à l'OFDF[28] de bien vouloir lui transmettre les éléments que ces offices avaient transférés au PFPDT en lien avec Xplain et qui pourraient présenter un intérêt pour l'enquête administrative.

17 Du 14 novembre 2023 au 14 décembre 2023, OA a conduit des interrogatoires à Berne.

18 A compter du 21 novembre 2023, OA a disposé d'un accès complet aux données Exchange extraites par les prestataires internes de services informatiques de la Confédération, triées par l'AFC selon les critères fournis par OA et mises à disposition de OA sur la plateforme *Nuix Investigate*.

19 Le 18 décembre 2023, OA a envoyé à fedpol une demande de renseignements tendant à la production de tout contrat avec Xplain AG relatif au projet ORMA et antérieur à 2011, dès lors qu'aucun contrat relatif au projet ORMA antérieur à 2011 n'avait été remis jusqu'alors à OA[29].

20 Le 18 décembre 2023, OA a transmis au Secrétariat Général du DFF une synthèse de ses constatations au 15 décembre 2023[30].

21 En janvier-février 2024, OA a conduit de nouveaux interrogatoires qui se sont achevés le 9 février 2024, totalisant ainsi 32 interrogatoires à Berne (à savoir 30 employés de la Confédération et deux personnes tierces).

---

[21] Le masculin générique est ponctuellement utilisé dans ce document à des fins de lisibilité.
[22] AUD 03.06.02.27-38 et B03.06.02.04.
[23] AUD 03.05.02.13-19 et B03.05.02.03
[24] AUD 03.02.39-43 et B03.02.31.
[25] Cf. à ce sujet, *infra* par. 43-49.
[26] AUD 03.02.68-72 ; AUD 03.05.02.23-27 ; AUD 03.06.02.40-44.
[27] AUD 03.04.01.17-19.
[28] AUD 03.06.01.9-11.
[29] AUD 03.04.01.22-24.
[30] AUD 01.02.514-515 et B01.02.91-92.

22 Le 1er mars 2024, l'Organe d'enquête a remis un projet de rapport à l'Organe de coordination afin de permettre l'exercice par les Unités touchées par l'enquête de leur droit d'être entendu (art. 27*g* al. 5 OLOGA). Ce dernier l'a transmis le même jour aux Unités touchées par l'enquête en les invitant à adresser à l'Organe d'enquête toute demande d'accès au dossier et toute prise de position sur le projet de rapport. L'Organe d'enquête a analysé toutes les prises de position reçues. Des précisions ont été apportées dans le présent rapport, dans la mesure nécessaire.

23 Entre le 5 et le 12 mars 2024, l'Organe d'enquête a contacté les employés de la Confédération au sujet desquels le projet de rapport du 1er mars 2024 contient des constatations[31]. Ces personnes ont reçu les passages du projet de rapport qui les concernent (art. 27*g* al. 4 et 5 OLOGA). Le reste du document était caviardé. Elles ont été invitées à adresser à l'Organe d'enquête toute éventuelle demande d'accès au dossier ou prise de position. L'Organe d'enquête a analysé toutes les prises de position reçues. Des précisions ont été apportées dans le présent rapport, dans la mesure nécessaire.

B. Mesures immédiates recommandées

24 Selon le contrat de mandat, OA devait signaler sans retard à l'Organe de coordination les situations qui appellent des mesures immédiates (*Sofortmassnahmen*) y compris les indices de fautes individuelles (*individuelle Fehler*).

1. « *Error-Reporting* »

25 En application de la clause précitée et par e-mail chiffré du 1er décembre 2023, OA a signalé à l'Organe de coordination un mécanisme dit de « *Error-Reporting* » susceptible d'avoir conduit à des transferts de données productives de l'administration fédérale vers Xplain. OA précisait que ce mécanisme aurait été mis en place pour tous les clients de Xplain et ne concernerait donc pas uniquement l'administration fédérale.

26 L'Organe de coordination a indiqué à OA avoir transmis ces informations aux unités concernées. Selon les informations communiquées par l'Organe de coordination, la fonctionnalité de *Error-Reporting* a été désactivée en été 2023. Les directives internes ont été adaptées et les produits (*software*) concernés sont en cours de mise à jour afin de supprimer définitivement la fonctionnalité.

2. Fautes individuelles

27 En application de la clause précitée et par e-mail chiffré du 1er décembre 2023, OA a indiqué à l'Organe de coordination avoir identifié un collaborateur de fedpol et un collaborateur de l'OFJ ayant adressé à Xplain, par e-mail(s) apparemment non chiffré(s), des données productives de leur unité administrative.

28 De même, par e-mail chiffré du 2 février 2024, OA a indiqué à l'Organe de coordination avoir identifié un collaborateur de la BAC ayant adressé par e-mail à Xplain des données productives d'une unité administrative.

29 Enfin, par e-mail chiffré du 28 février 2024, OA a transmis à l'Organe de coordination des éléments découverts fortuitement suggérant qu'un employé de fedpol pourrait avoir demandé certains privilèges aux administrateurs de Xplain à quatre occasions entre 2009 et 2014[32].

[31] Un ancien employé de la Confédération a également été contacté.
[32] Cf. *infra* par. 560.

C. Principaux moyens de preuve

30 Les principaux moyens de preuve réunis au cours de l'enquête sont les suivants :

- Contrats remis par les Unités touchées par l'enquête suite aux demandes de renseignements du 4 septembre 2023 ;
- Directives et documents analogues remis suite aux demandes de renseignements du 4 septembre 2023 ;
- 32 interrogatoires à Berne (30 employés de la Confédération ; deux personnes tierces), entre le 14 novembre 2023 et le 9 février 2024 ;
- Documents et informations remis par fedpol et l'OFDF au PFPDT et transmis à OA à sa demande ;
- Rapport du NCSC du 14 décembre 2023 sur la cyberattaque ayant touchée Xplain[33] ;
- Projet du SEPOS d'état des lieux relatif à la question de la sécurité de la chaîne d'approvisionnement à la lumière de la loi sur l'information, daté du 22 janvier 2024 et transmis spontanément par le SG-DFF le 23 janvier 2024[34].

31 En outre, les données électroniques suivantes ont été mises à disposition de l'Organe d'enquête en vue de leur tri et du versement éventuel au dossier de l'enquête des éléments potentiellement pertinents :

- Copie du *Datendump* (1'295'862 éléments), comprenant les *tags* du NCSC (identifiant en particulier les données de la Confédération)[35], mise à disposition d'OA sur la plateforme *Nuix Investigate* (le « ***Datendump*** ») ;
- Données Exchange (2'719'026 éléments), mises à disposition d'OA sur la plateforme *Nuix Investigate* comme suite à ses demandes (les « **Données Exchange** »).

32 Après avoir été convoqués par e-mail à leur adresse professionnelle et informés sur leurs droits et obligations[36] ainsi que sur les règles de procédure appliquées par l'Organe d'enquête[37], les employés suivants de la Confédération ont été interrogés par OA à Berne (par ordre alphabétique de l'employeur actuel)[38] :

Employeur au moment de l'interrogatoire	Niveau hiérarchique – type de responsabilités	Précédent employeur au sujet duquel des questions ont été posées
armasuisse	Direction	-
BAC	Direction	-

[33] « *Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain* » (AUD 01.02.520 et AUD B01.02.93).
[34] « *Auslegeordnung zur Supply Chain Security im Lichte des Informationssicherheitsgesetzes unter Berücksichtigung weiterer Modelle und der getroffenen Massnahmen*».
[35] D'après le NCSC, sur un total de 64'923 objets pertinents (c'est-à-dire après exclusion notamment des *backups,* fichiers système, composants standards et doublons), 9'040 objets peuvent être attribués à la Confédération en tant que « *Dateneigentümerin* ». Sur ces 9'040 objets, le NCSC retient que 95.17% sont des objets du DFJP, 3.38% du DDPS, 0.76% du DEFR, 0.61 % du DFF, 0.07% du DFI et 0.01% du DFAE.
[36] Notamment le droit de ne pas s'incriminer (*nemo tenetur* ; art. 27*h* al. 2 OLOGA).
[37] AUD B01.02.65.
[38] Le terme « responsable » comprend ici notamment la fonction de « Chef/Cheffe ».

Employeur au moment de l'interrogatoire	Niveau hiérarchique – type de responsabilités	Précédent employeur au sujet duquel des questions ont été posées
Cdmt des Opérations	Direction	-
Cdmt des Opérations	Responsable Informatique et cybersécurité	-
DFAE	Direction	-
fedpol	Délégué à la sécurité informatique	-
fedpol	Direction	-
fedpol	Business Analyst	-
fedpol	Responsable de projet	OFDF
fedpol	Responsable de projet	-
NCSC	Responsable Vulnérabilités	-
OFCL	Direction	-
OFDF	Direction	-
OFDF	Délégué à la sécurité informatique	-
OFDF	Délégué à la sécurité informatique	-
OFIT	Responsable de projet	CSI-DFJP
OFJ	Responsable d'application	CSI-DFJP
OFJ	Responsable IT / Délégué à la sécurité informatique	-
OFJ	Responsable RI / Responsable de projet	-
OFJ	Direction	-
PM	Responsable d'un domaine de base de conduite	-
SEM	Direction	-
SEM	Assistance scientifique	OFDF
SEM	Senior Business Analyst/Product Owner	-
SEM	Responsable Sécurité informatique, bureautique et infrastructure	OFDF
SEM	Délégué à la sécurité informatique	-
SEM	Responsable Planification et ressources	-
SEPOS	Secrétaire d'Etat	-
SRC	Responsable Cyber	-

33 En outre, le responsable du Service pour la sécurité de l'information du SEPOS a accompagné le Secrétaire d'Etat à la politique de sécurité lors de l'interrogatoire de ce dernier.

34 Conformément à la décision du Conseil fédéral du 23 août 2023, les employés et mandataires actuels et anciens de la Confédération ont été libérés du secret professionnel, du secret d'affaires et du secret de fonction à l'égard de OA en tant qu'organe chargé de l'enquête pour la durée de l'enquête pour toutes les informations qui se rapportent à l'objet de l'enquête.

35 Au vu du contenu des interventions faites par ces personnes dans les médias au sujet de la relation entre la Confédération et Xplain, les personnes suivantes ont été entendues en qualité de tiers (par ordre alphabétique) :

- Christian FOLINI, Ingénieur en sécurité informatique et auteur dans ce domaine ;
- Matthias STÜRMER, Professeur à la Haute école spécialisée bernoise (*Berner Fachhochschule*), directeur de l'Institut *Public Sector Transformation*, spécialisé en matière de digitalisation en particulier dans le secteur public.

36 MM. FOLINI et STÜRMER ont été convoqués par e-mail à leur adresse professionnelle et informés sur leurs droits et obligations[39] ainsi que sur les règles de procédure appliquées par l'Organe d'enquête[40].

37 Tous les interrogatoires ont été enregistrés (son uniquement), avec, dans chaque cas, l'accord de la personne entendue. Un procès-verbal a été établi par OA séance tenante et signé par chaque personne entendue. Ce procès-verbal contient uniquement les informations formelles communiquées en début d'interrogatoire (objet, droits et obligations). Par ailleurs, OA a établi une transcription *verbatim* de chaque enregistrement sonore, étant précisé que l'enregistrement fait foi. Les enregistrements, procès-verbaux et transcriptions ont été versés au dossier de l'enquête[41].

D. Coopération

38 L'Organe d'enquête tient à souligner la qualité de la coopération des Unités touchées par l'enquête, des secrétariats généraux des départements concernés, ainsi que de toutes les personnes qui ont été interrogées. Il a été donné suite à toutes les demandes d'OA et les délais impartis par OA, qui étaient particulièrement brefs au vu de la nécessité de respecter le calendrier d'enquête décidé par le Conseil fédéral (cf. *supra* par. 2), ont été respectés.

39 OA relève également que la coopération avec les unités impliquées dans le processus de mise à disposition des données Exchange de la Confédération (cf. *infra* E.1) s'est avérée particulièrement constructive, compte tenu des défis techniques (capacité du *hardware* et du *software* à fonctionner sous tension) qu'il a fallu affronter dans des délais spécialement courts. L'engagement de l'OFIT et de l'AFC s'est révélé décisif dans ce contexte.

40 OA salue également l'excellente coopération avec l'Organe de coordination et le Groupe de travail mis en place par le DFF, ainsi que le soutien reçu. OA note que son indépendance a été respectée en tout temps.

41 Il peut tout au plus être relevé qu'OA a reçu relativement peu d'informations de manière spontanée de la part des Unités touchées par l'enquête, directement ou via l'Organe de coordination. Or, au moment où le mandat a débuté le 1er septembre 2023, les Unités touchées par l'enquête avaient connaissance de la Fuite de données depuis plusieurs mois et des démarches de clarifications internes des faits avaient été menées, à tout le moins par certaines d'entre elles, comme l'ont montré les interrogatoires menés ensuite par OA.

42 L'Organe d'enquête a en revanche reçu du Contrôle fédéral des finances (CDF), en septembre 2023, deux déclarations de soupçon provenant de lanceurs d'alerte anonyme (*whistleblowers*), dont il a été tenu compte dans l'enquête. Celles-ci ne contenaient pas d'éléments décisifs.

[39] Ces personnes ont notamment été informées de leur droit de refuser de témoigner (art. 27*h* al. 3 OLOGA).
[40] AUD 04.02.1-6; B01.02.65; B04.02.01 / AUD 04.03.1-6; B01.02.65; B04.03.01.
[41] Rubrique 4 du dossier.

E. Limitations

1. Exhaustivité des données Exchange

43 Dès le début de l'enquête, OA a signalé à l'Organe de coordination sa volonté de procéder à une analyse forensique de données de messagerie de la Confédération (notamment e-mails et entrées de calendrier). L'OFIT a proactivement soutenu OA notamment dans la phase préalable à l'extraction de données en analysant les variantes techniques permettant d'identifier des données pertinentes.

44 Ces analyses, auxquelles s'ajoutaient des considérations juridiques (notamment le respect du principe de proportionnalité), ont conduit OA à exclure l'hypothèse d'une extraction de l'intégralité des boîtes de messagerie de toutes les Unités touchées par l'enquête selon les informations fournies par ces dernières. Selon les estimations de l'OFIT, l'extraction d'un tel volume de données représentait un temps technique de près de deux mois.

45 OA s'est donc fondée sur les listes de personnes potentiellement pertinentes que les Unités touchées par l'enquête lui ont remises à sa demande pour définir le cercle des boîtes de messagerie devant être extraites. En outre, OA a demandé aux Unités touchées par l'enquête[42] d'identifier les boîtes de messagerie de personnes appartenant à certains secteurs (Direction ; Juridique ; Achats ; si applicable : Informatique) au cours d'une certaine période temporelle. Enfin, OA a demandé aux Unités touchées par l'enquête d'identifier tous les organes, employés ou mandataires de Xplain disposant ou ayant disposé d'un compte de messagerie de l'unité concernée, d'un accès à un compte de messagerie d'un employé de l'unité concernée, d'un accès à un compte commun/partagé de messagerie de l'unité concernée ou qui recevait/reçoit des messages automatiquement redirigés par un compte de messagerie de l'unité concernée.

46 OA a ensuite adressé des demandes à l'OFIT, à la BAC et à l'unité Informatique du DFAE visant à (i) l'extraction des données de messagerie sélectionnées, (ii) le tri de ces données selon des critères de recherche définis par OA et (iii) la mise à disposition de ces données sur la plateforme *Nuix Investigate* exploitée par l'AFC.

47 Après analyse de ces données, l'Organe d'enquête n'a versé au dossier (art. 27*j* al. 1 OLOGA) que les éléments (i) qui paraissent pertinents pour l'enquête, excluant notamment tout ce qui relève de la sphère privée des personnes concernées, et (ii) qui ne sont pas protégés par le secret professionnel de l'avocat (cf. art. 13 al. 1bis PA).

48 La méthode procède ainsi d'un arbitrage entre les règles juridiques applicables (en particulier la proportionnalité), l'intérêt de l'enquête (en particulier la recherche de la vérité) et les contraintes temporelles (en particulier les délais impartis à l'Organe d'enquête).

49 L'exhaustivité des recherches dans les données de messagerie ne peut donc pas être garantie.

2. Absence d'obligation de coopérer des tiers

50 L'absence d'obligation de coopérer des tiers est une limite inhérente à toute enquête administrative selon les art. 27*a* ss OLOGA (cf. art. 27*h* al. 3 OLOGA). En l'espèce, elle a constitué un obstacle à l'établissement des faits à plusieurs titres.

[42] A l'exception du DFAE, qui n'était concerné que par le second aspect de cette demande (contacts avec Xplain).

51 Ainsi, par courrier du 19 septembre 2023, Xplain a refusé de fournir les renseignements et documents sollicités par OA le 6 septembre 2023[43].

52 Par ailleurs, aucun des sept employés de Xplain qui ont été contactés, ni l'ancien CEO de cette société, n'ont répondu aux sollicitations d'OA pour un interrogatoire.

53 Enfin, un ancien cadre de fedpol (2002-2018), contacté par OA par courrier grâce aux indications données par fedpol, a refusé de donner suite à sa convocation pour un interrogatoire[44]. Comme souligné en doctrine, il faut considérer les anciens employés comme des tiers, qui n'ont pas l'obligation de coopérer (cf. art. 27*g* al. 2 *a contrario* et art. 27*h* al. 3 OLOGA)[45].

3. Refus du PFPDT de remettre des documents et informations

54 Le 15 septembre 2023, OA a adressé une demande de renseignements au Préposé fédéral à la protection des données et à la transparence (« PFPDT »).

55 Le 12 octobre 2023, OA a demandé au PFPDT s'il était disposé à collaborer en tant que tiers, vu le refus opposé par celui-ci à la première demande de renseignements de OA.

56 Par courrier du 18 octobre 2023, le PFPDT a indiqué souhaiter préserver « *sa pleine marge de manœuvre et une indépendance complète* » et a, substance, refusé de remettre les documents et informations sollicités par OA.

4. Décision du Tribunal pénal fédéral relative à l'entraide avec le Ministère public de la Confédération

57 Le 6 septembre 2023, OA a adressé une demande d'accès au dossier au Ministère public de la Confédération (« MPC »)[46].

58 Par décision du 7 décembre 2023, la Cour des plaintes du Tribunal pénal fédéral a admis un recours de Xplain et a annulé l'ordonnance du MPC du 10 octobre 2023 octroyant à OA l'accès au dossier de la procédure pénale[47]. Aucune voie de droit ordinaire n'existe contre cette décision.

59 Par conséquent, OA n'a pas eu accès aux informations et moyens de preuve potentiellement pertinents en mains du MPC.

5. Absence de moyens légaux pour localiser les anciens employés

60 Les moyens à disposition de l'organe d'enquête selon les art. 27*a* ss OLOGA sont limités s'agissant de la localisation de personnes qui ne sont plus employées par l'administration fédérale. Lorsque la dernière unité de l'administration fédérale auprès de laquelle une personne était employée ne dispose pas d'information à cet égard, OA en tant qu'organe d'enquête ne dispose d'aucun moyen autre que la consultation de sources publiquement accessibles pour tenter de localiser cet ancien employé.

61 Ainsi, un ancien employé d'armasuisse qu'OA souhaitait interroger n'a pas pu être localisé.

---

[43] AUD 03.09.1-5.
[44] AUD 04.41.19.
[45] BERNHARD RÜDY, in ASDPO Association suisse du droit public de l'organisation (éd.), Verwaltungsorganisationsrecht - Staatshaftungsrecht- öffentliches Dienstrecht, 2013, p. 128.
[46] AUD 07.01.1-2.
[47] Décision BB.2023.181 du 7 décembre 2023.

IV. FAITS ETABLIS PAR L'ENQUETE

A. Données productives en possession d'Xplain AG

62 Conformément au contrat du 24 août 2023 et au mandat du Conseil fédéral du 23 août 2023, l'enquête visait notamment à déterminer les circonstances de fait qui ont conduit à ce que des données productives de la Confédération soient présentes dans l'environnement informatique de Xplain.

63 Le droit fédéral ne définit pas la notion de « données productives ». En référence au Message du Conseil fédéral concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités du 4 mars 2022[48], nous entendons par « **données productives** » de la Confédération :

> *Les données réelles issues des systèmes d'information de la Confédération, par opposition aux données tests ou anonymisées.*

64 Au vu notamment des explications reçues du NCSC lors de la séance du 4 septembre 2023 avec l'Organe de coordination et le groupe de travail, les hypothèses de travail suivantes ont été formulées par OA :

1) Des collaborateurs de Xplain disposaient/disposent de boîtes e-mail de la Confédération et se sont transférés à leur adresse Xplain des données productives de la Confédération (hypothèse « *forward* »).
2) Des collaborateurs de Xplain disposaient/disposent d'accès à des systèmes de la Confédération qui ont permis le transfert de données productives vers l'environnement informatique de Xplain (hypothèse « **accès** »).
3) Des collaborateurs de la Confédération ont transmis activement des données productives de la Confédération à des collaborateurs de Xplain (hypothèse « **transfert actif** »).
4) Des mécanismes automatiques ont conduit au transfert de données productives vers l'environnement informatique de Xplain (hypothèse « **transfert automatique** »).

65 Nous avons cherché à vérifier ces hypothèses à en les confrontant aux moyens de preuve réunis en cours d'enquête, soit en particulier le *Datendump* ainsi que les Données Exchange mises à notre disposition.

66 Les hypothèses « *forward* », « accès » et « transfert actif » sont confirmées. L'hypothèse « transfert automatique » n'est pas confirmée ; un mécanisme qui pourrait être qualifié de « semi-automatique » a toutefois été identifié (ci-dessous ch. 9).

67 Nous n'avons pas identifié d'autres canaux ayant permis à des données productives de la Confédération d'entrer dans l'environnement informatique de Xplain.

68 Les cas présentés ci-dessous illustrent les canaux ainsi identifiés, à l'exception des cas n° 10 et 11 pour lesquels le canal est resté à ce jour indéterminé et qui sont mentionnés pour mémoire. Une partie de ces cas concernent des données productives dont la présence sur le darknet a été médiatisée en 2023 (ci-dessous ch. 1, 2, 7). D'autres ont été identifiés par l'enquête (ci-dessous ch. 3, 4, 5, 6, 8, 9).

69 Compte tenu des limitations décrites plus haut, l'analyse qui suit n'est pas exhaustive.

[48] Message concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités du 4 mars 2022, FF 2022 804, p. 85

1. Cas de forward n° 1 : un tableur Excel (extraction ORMA) contenant des détails sur des enquêtes pénales et des procédures d'entraide pénale (fedpol) (16 septembre 2020)

70 L'hypothèse du forward s'est vérifiée. Elle est illustrée en particulier par le présent cas.

71 Le contexte est le suivant : un employé fedpol (« A ») adresse un e-mail le 11 août 2020 à un autre employé fedpol (« B ») en lui demandant si Xplain a pu répondre à une interrogation relative à des inscriptions manquantes dans un fichier exporté (« *Hast du inzwischen seitens xPlain eine Rückmeldung betreffend der fehlenden Einträge beim VASS Export erhalten?* »)[49].

72 VASS est l'abréviation de « *Verwaltung von Asservaten, Spuren und Spurenträgern*»[50].

73 Le 7 septembre 2020, B transmet à A, par e-mail chiffré, un fichier compressé nommé [redacted].zip[51].

74 Le 15 septembre 2020, A transfère ce fichier par e-mail à un employé d'Xplain (« Q »), à l'adresse [Q]@fedpol.admin.ch de ce dernier, en indiquant :

> *« Hallo [prénom de Q]*
>
> *Anbei das ZIP-File, welches ich am 07.09.2020 von [B] erhalten habe.*
>
> *Wie erwähnt, sind insbesondere die Spalten AJ – AQ leer. Dabei ist insbesondere die Spalte AP (ASSERVAT_SPEZ_BEZEICHNUNG) für mich Elementar.*
>
> *Ich benötige insbesondere folgende Spalten:*
>
> *D (ASSERVATEN_NR)*
>
> *E (SERIEN_NR)*
>
> *I (KATEGORIE)*
>
> *L (VASS_BESCHREIBUNG)*
>
> *V (AD_DOCTYPE)*
>
> *AJ (ASSERVAT_MARKE)*
>
> *AK (ASSERVAT_TYP)*
>
> *AL (ASSERVAT_SERIE_NR)*
>
> *AM (ASSERVAT_MENGE)*
>
> *AN (ASSERVAT_OERTLICHKEIT)*
>
> *AO (ASSERVAT_BEM)*
>
> *AP (ASSERVAT_SPEZ_BEZEICHNUNG)*
>
> *Für Fragen stehe ich dir gerne zur Verfügung ».*

75 Cet e-mail du 15 septembre 2020 figure dans des e-mails subséquents non chiffrés et le texte qu'il contenait est ainsi visible. Il n'y a pas d'indice que son texte ait été modifié dans les échanges

[49] AUD 03.10.03.2 et AUD 03.10.03.3.

[50] [redacted].pdf (29.08.2016) (AUD 03.10.09.157).

[51] L'existence de cet email a été signalée par B en mars 2024 dans le cadre du droit d'être entendu. Cet email ne figure pas dans les Données Exchange à disposition de l'Organe d'enquête.

subséquents. En revanche, l'e-mail original ne figure pas parmi les données à notre disposition, de sorte que nous n'avons pas pu établir s'il était chiffré ou non.

76 Le lendemain (16 septembre 2020), à 11h41, Q utilise son adresse [Q]@fedpol.admin.ch pour transférer à son adresse [Q]@xplain.ch l'e-mail précité reçu de A, avec en pièce jointe le fichier compressé précité[52].

77 Cet e-mail non chiffré ne contient pas de texte, mais uniquement la signature automatique suivante :

Mit freundlichen Grüssen
Meilleures salutations
Cordiali saluti
Best regards

Q [redacted]

Eidgenössisches Justiz- und Polizeidepartement - EJPD
Bundesamt für Polizei - fedpol
Direktionsbereich Polizeisysteme & Identifikation
Abteilung Polizei-Informationssysteme
Bereich Ermittlungssysteme

Guisanplatz 1a, 3003 Bern
Tel. +41 (0)58 [redacted]
Q [redacted]@fedpol.admin.ch
www.fedpol.ch

78 La pièce jointe est intitulée « [redacted].zip ». Ce fichier .zip représente environ 8 Mo. D'après ses métadonnées il a été créé le 7 septembre 2020.

79 Ce fichier compressé contient le fichier Excel intitulé « [redacted].xlsx ». Il s'agit d'un tableur comptant 39'938 lignes et une cinquantaine de colonnes. Ces lignes et colonnes contiennent des données sur des procédures pénales ou des procédures d'entraide internationale en matière pénale dans lesquelles fedpol est intervenue. Selon les cas, ce tableau mentionne tout ou partie des éléments suivants :

- Faits en cause,
- Numéro de procédure,
- Infractions soupçonnées,
- Noms et prénoms de personnes physiques, notamment de prévenus, de tiers saisis, d'enquêteurs de fedpol et de procureurs du Ministère public de la Confédération,
- Raisons sociales de personnes morales prévenues ou tierces,
- Actes d'entraide ou de procédure pénale effectués, notamment adresses auxquelles des perquisitions ont été menées,
- Pièces et objets mis en sûreté ou séquestrés,

[52] AUD 03.10.03.1.

80 Environ deux heures plus tard (16 septembre 2020, 13h33), Q envoie depuis son adresse [Q]@xplain.ch un e-mail non chiffré à un collaborateur du CSI-DFJP (« C »). A et B sont en copie. En annexe à son e-mail, Q joint un fichier « [redacted].sql » et il indique dans le texte de l'e-mail :

> *« Hallo [prénom de C],*
>
> *darf ich Dich bitten, auf der ORMA Produktion das angehängte Statement auszuführen und das Resultat als Excel an [A]@fedpol.admin.ch zu senden.*
>
> *Die Liste enthält die von [surnom de A] gewünschten Spalten, ohne die Verbindung auf die Sicherstellung zu machen.*
>
> *Danke.»*

81 Ce fichier .sql contient 46 lignes de code. Il s'agit d'informations techniques. Aucune des données précitées qui étaient contenues dans le fichier Excel ne figurent dans ce fichier .sql.

82 Environ 45 minutes plus tard (16 septembre 2020, 14h16), C envoie un e-mail chiffré à A, dont le sujet est le même que l'e-mail du même jour que C a reçu de Q. L'Organe d'enquête n'est pas en mesure de déchiffrer ce message.

83 Le lendemain (17 septembre 2020), A envoie un e-mail non chiffré à Q à son adresse [Q]@xplain.ch dans lequel il indique que C lui a envoyé hier le tableur Excel. A remercie Q pour son aide.

84 Le fichier [redacted].xlsx fait partie des données de Xplain qui ont été mises en ligne sur le darknet en juin 2023. D'après les métadonnées du fichier trouvé dans le Datendump, ce fichier se trouvait dans l'environnement informatique de Xplain dans un *User Share* portant le prénom de Q [53].

2. Cas de forward n° 2 : divers fichiers joints à un e-mail, contenant notamment des informations classifiées sur les conseillers fédéraux et des fonctionnaires étrangers (5 mai 2018)

85 Le contexte est le suivant : le 1er mai 2018 à 14h53, un employé de fedpol (« D ») envoie depuis son adresse [D]@fedpol.admin.ch un e-mail à un employé de Xplain (« R ») à son adresse [R]@fedpol.admin.ch, intitulé « [redacted] » et comprenant le texte suivant :

> *« Sehr geehrt[*] [nom de D]*
>
> *Anbei sende ich Ihnen die versprochenen Unterlagen. Die vier jpg's zeigen Ausschnitte unserer jetzigen Ablage.*
>
> *Vergessen wurde, dass wir monatlich Sicherheitsmassnahmen der diplomatischen Vertretungen an diverse Kantone versenden (siehe [redacted].pdf). In diesen Schreiben geht es darum, eine vorgefertigte Excel-Tabelle einzufügen.*
>
> *Bei Fragen stehen wir Ihnen gerne zur Verfügung »*[54]*.*

86 Quatre personnes, apparemment des employés de fedpol, sont en copie de cet e-mail (à destination de leur adresse @fedpol.admin.ch).

87 Cet e-mail est chiffré et l'Organe d'enquête n'est pas en mesure de le déchiffrer. Son texte figure dans un e-mail subséquent du 18 mai 2018 à 16h05. Il n'y a pas d'indice que le texte d'origine ait été modifié dans cet e-mail subséquent.

---

[53] Path name: […]/XPLAIN/User Shares/[prénom de X].
[54] AUD 03.10.04.1.

88 Ainsi, le 18 mai 2018 à 16h05, R transfère, sans texte ni signature automatique, l'e-mail précité du 1er mai 2018 et ses annexes depuis son adresse [R]@fedpol.admin.ch vers son adresse [R]@xplain.ch. Le sujet de l'e-mail est « WG: [redacted] ».

89 Parmi les 11 annexes à cet e-mail, six portent la mention CONFIDENTIEL (« *VERTRAULICH* ») et datent de fin 2017 respectivement début 2018. Il s'agit de documents (format .pdf) de fedpol destinés à des polices cantonales et relatifs à des rencontres (réception, arrivée, rendez-vous) impliquant des haut-fonctionnaires nationaux et internationaux.

90 Les annexes contiennent notamment un fichier « [redacted].pdf », dont le contenu est classifié CONFIDENTIEL, contenant des informations relatives à des conseillers fédéraux.

91 Par ailleurs, les documents annexés à l'e-mail du 18 mai 2018 précité contiennent les types d'informations suivants :

- Mesures de sécurité en faveur de personnel diplomatique et d'ambassades étrangères, y compris des numéros de téléphone portable d'employés de fedpol ;
- Programmes de manifestations dans des ambassades ; et
- Escortes de personnel de la protection diplomatique.

92 Enfin, une capture d'écran montre une partie de l'arborescence du disque Fedpol-Org (O:).

3. Cas de forward n° 3 : l'envoi d'un tableur Excel contenant plus de 1'000 lignes relatives à des notices Interpol (1er septembre 2021)

93 Le 1er septembre 2021 à 11h54, un employé de Xplain (« Z ») envoie un e-mail non chiffré intitulé « [redacted] » à un employé de Xplain (« W »), à la fois sur son adresse [W]@fedpol.admin.ch et sur son adresse [W]@xplain.ch.

94 Z indique ce qui suit :

> *« Hallo [prénom de W]*
>
> *Kannst Du das Select Skript für die Meldungen gemäss Excel ausführen. Und dann auf blockiert Zuteilungen untersuchen.*
>
> *Aber noch kein Update Script ausführen.*
>
> *Gruss [prénom de Z] ».*

95 L'e-mail contient en pièce jointe un fichier « [redacted].*xlsx* ». Les 1'045 lignes de ce tableur contiennent des informations relatives à des notices Interpol de différentes catégories, soit des notices rouges, bleues ou jaunes, dans 32 colonnes, dont les suivantes :

- Degré d'urgence (« *Dringlichkeit* ») ;
- Numéro d'annonce (« *Meldungsnummer* ») ;
- Type d'annonce (« *Meldungstyp* ») ;
- Date d'entrée de l'annonce (« *Datum Eingang* ») ;
- Autorité requérante (« *Absender* ») ;
- Référence (« *Referenz* ») ;
- Commentaire (« *Bemerkung* »).

96 La colonne « *Bemerkung* » contient des informations relatives à des personnes physiques dans 785 lignes. Ces personnes sont selon toute vraisemblance visées ou citées dans la notice Interpol correspondante. Selon les cas, ces informations contiennent les éléments suivants :

- Nom et prénom ;
- Sexe ;
- Date de naissance ;
- Nationalité ;
- Hyperlien vers la notice Interpol ;
- Le cas échéant, le motif de l'annonce (p. ex. : « *extradited* »).

97 L'enquête n'a pas permis de déterminer si Z a préalablement reçu d'un employé fedpol le fichier Excel en question ou si Z lui-même a procédé à une extraction de données du système de production ORMA et dans cette hypothèse dans quelles circonstances.

98 Deux jours plus tard, le 3 septembre 2021 à 9h49, W envoie un e-mail intitulé « [redacted] *.xlsx* [redacted] » depuis son adresse [W]@fedpol.admin.ch à son adresse [W]@xplain.ch ainsi qu'à celle d'un autre employé de Xplain (« X » ; [X]@xplain.ch)[55].

99 L'e-mail ne contient aucun texte.

100 L'e-mail contient en pièce jointe un fichier Excel intitulé « [redacted] *.xlsx* »[56]. Il s'agit d'un tableur contenant 228 lignes, qui reprennent une partie des 1'045 lignes du fichier « [redacted] .xlsx ». Le tableur compte au surplus les mêmes 32 colonnes que le fichier précité.

4. Cas d'accès : un tableur Excel (extraction ORMA) contenant le « Betreff » des affaires (22 septembre 2011)

101 L'hypothèse de l'accès s'est également vérifiée, à tout le moins concernant fedpol. L'Organe d'enquête n'a pas identifié de cas d'accès concernant les autres Unités directement concernées.

102 Le contexte est le suivant : fedpol exploite plusieurs systèmes d'informations de police au sens des art. 9 ss LSIP, lesquelles contiennent des données traitées par les autorités fédérales et cantonales en matière de poursuite pénale, de police et de sécurité intérieure.

103 Au cours de la période sous enquête, ORMA constituait la solution informatique de fedpol pour le système informatisé de gestion interne des affaires et des dossiers, soit la catégorie de « Gestion des affaires et des dossiers » (« GA ») au sens de l'art. 18 LSIP[57]. L'application constitue la sous-catégorie de gestion des affaires en particulier pour les systèmes d'informations JANUS (désormais : « SNE » ; art. 5 let. d de l'Ordonnance SNE) et IPAS de fedpol (art. 5 Ordonnance IPAS)[58].

104 Les données relatives à la sous-catégorie GA de JANUS et IPAS doivent en principe être effacées à l'échéance d'un délai de conservation de trois ans, à moins qu'elles ne présentent un lien avec un autre sous-système ou une autre sous-catégorie (art. 22 al. 6 de l'Ordonnance SNE ; art. 9 al. 8 de l'Ordonnance IPAS).

[55] AUD 03.10.06.1.
[56] AUD B03.10.06.01.
[57] AUD B03.04.10.1261.
[58] Chiffre 8 al. 2 let. d Bearbeitungsreglement IPAS (AUD B03.03.10.886) ; Chiffre 27 al. 1 Bearbeitungsreglement JANUS (AUD B03.04.10.975)

105 Le 2 septembre 2010 à 11h01, un employé de fedpol (« E ») envoie à un autre employé de fedpol (« F ») un e-mail non chiffré intitulé « [redacted] »[59]. E indique que, comme annoncé oralement, en vue d'un effacement ORMA à venir (« *die bevorstehende ORMA Löschung* »), il a besoin d'une liste avec les critères suivants :

> • *ORMA-Meldungen, vor dem 1.7.2007 erfasst und keinem Dossier zugeteilt (Feld Dossier = leer)*
>
> • *Meldungen und PR (keine EP)*

106 E demande à F de lui envoyer une telle liste en format Excel, « *[a]nalog der Auswertung aus dem Jahr 2008* ». E indique au surplus :

> *« Nach erhalt der Liste werde ich diverse Daten sichten und prüfen, evtl. werde ich mich erneut mit Dir in Verbindung setzen.*
>
> *Danach werden die Abteilungen informiert und gebeten, die Daten zu prüfen und wenn nötig mit dem fehlenden Dossier zu ergänzen, damit diese nicht gelöscht werden. Nicht bearbeitete Meldungen werden gemäss Janus VO Art. 22, Abs. 6 nach 3 Jahren ab deren Erfassung gelöscht.»*

107 Une heure plus tard, soit le 2 septembre 2010 à 12h04, F transfère l'e-mail précité à un employé de Xplain (« S »), à son adresse [S]@xplain.ch, et lui demande ce qui suit [60]:

> *« Tschou [surnom de S]*
>
> *Dies wäre ein weiterer Task für nach Deinen Ferien.*
>
> *Bitte wie im Jahr 2008 dies mittels Skript auf der DB abschecken und die Ausgabe als Excel file zustellen. Bitte bis 20.09.2010 Feedback an [E] und mich ein "cc" senden.*
>
> *Gruess »*

108 Environ deux semaines plus tard, le 17 septembre 2010, S envoie un e-mail non chiffré à E, avec F en copie, depuis son adresse [S]@xplain.ch.

109 S indique ce qui suit[61] :

> *« Hallo [prénom de E],*
>
> *Im Anhang sende ich Dir die gewünschte Liste.*
>
> *Bei Fragen, bin ich nächsten Mittwoch wieder bei Fedpol erreichbar. Tel direkt: [*****]*
>
> *Grüsse,*
>
> *[prénom de S]»*

110 L'e-mail non chiffré envoyé par S depuis l'environnement informatique de Xplain contient deux pièces jointes :

- Un tableur Excel intitulé « [redacted]*.xls* »[62], et

[59] AUD 03.10.02.1.
[60] AUD 03.10.02.3.
[61] AUD 03.10.02.6.
[62] AUD B03.10.02.01.

- Un document intitulé « [redacted].*pdf* »[63], à l'en-tête de fedpol.

111 En substance, le tableur Excel « [redacted].*xls* » contient une colonne C intitulée « *Betreff* » avec 8'446 lignes d'informations relatives à diverses procédures, notamment pénales, dans lesquelles fedpol est intervenue, soit selon les cas :

- Nom ou prénom des personnes physiques impliquées dans les procédures (en tant que prévenu notamment) ;
- Infraction reprochée ;
- Numéros de téléphone ;
- Adresses e-mail ;
- Mesures d'enquête effectuées par fedpol.

112 Le fichier contient également une colonne « *Meldungs Nr und Kurzauskunft* », laquelle indique le numéro d'annonce ainsi que divers renseignements y relatifs, à savoir notamment les autorités nationales et étrangères impliquées, l'implication éventuelle d'Interpol, et les dates concernées.

113 Interrogé à ce sujet par l'Organe d'enquête, F a indiqué que, dans le cadre de ces travaux d'effacements de données ORMA, seul le numéro d'annonce (*Meldungsnummer*) était nécessaire au travail effectué par S : « *Und eben, die Löscharbeiten… [E] war jahrelang auch beim Kontrolldienst tätig, und sie haben uns gesagt, das, das, das muss gelöscht werden. Und da musste [S] auf die Datenbank ein Skript erstellen, das heisst für ihm relevant war natürlich die Nummer. Der Betreff war ihm eigentlich egal. Also es kam auch auf keinem Skript darauf*. »[64].

114 L'Organe d'enquête déduit des éléments qui précèdent que S, un employé de Xplain, disposait au moment des faits (septembre 2010) d'un accès au système de production ORMA de fedpol, qui lui a permis d'extraire des données de ce système. Dans des circonstances factuelles que l'enquête n'a pas permis de clarifier définitivement, un fichier Excel contenant des données de ORMA production extraites par S à la demande de F (employé de fedpol) s'est trouvé dans l'environnement informatique de Xplain. Puis, S a envoyé ce fichier par e-mail non chiffré depuis son adresse [S]@xplain.ch à des employés de fedpol à leur adresse @fedpol.admin.ch.

115 Par ailleurs, au vu des déclarations de F et s'agissant de travaux d'effacement périodiques, il n'est pas exclu que les faits décrits ci-dessus se soient également produits lors de l'effacement des données ORMA avant ou après 2010. Nous n'avons toutefois pas identifié, sur la base des Données Exchange, d'autres e-mails de S contenant une annexe comparable à celle décrite au paragraphe 111.

5. Cas de transfert actif n° 1 : des captures d'écran envoyées dans le cadre de la migration PAGIRUS-TROVA (28 janvier 2016)

116 L'hypothèse du transfert actif s'est aussi vérifiée. Elle est illustrée notamment par le présent cas.

117 Le contexte est le suivant : un employé de l'OFJ (« G ») a envoyé le 28 janvier 2016 à 10h50, depuis son adresse [G]@bj.admin.ch, un e-mail non chiffré intitulé « [redacted] » à un employé de Xplain (« T »), sur son adresse [T]@xplain.ch, et à une personne externe à la

[63] AUD B03.10.02.08.
[64] Enregistrement audio de l'interrogatoire n° 231129-000, à partir de 1'07'15.

Confédération (« P » ; [P]@[***].ch). Selon son site internet, P offre des services de consultant en informatique. Deux employés de l'OFJ sont en copie[65].

118 L'e-mail en question a été envoyé dans le cadre de la migration de données du système PAGIRUS vers TROVA (« [redacted] *Bei Fragen stehen wir gerne zur Verfügung* »).

119 L'e-mail en question contient 14 pièces jointes en format Word, ayant les intitulés suivants :

- [redacted].docx[66]
- [redacted]docx[67]
- [redacted]doc[68]
- [redacted]doc[69]
- [redacted]doc[70]
- [redacted]doc[71]
- [redacted]doc[72]
- [redacted]doc[73]
- [redacted]docx[74]
- [redacted].doc[75]
- [redacted].doc[76]
- [redacted]docx[77]
- [redacted]docx[78]
- [redacted]doc[79]

120 Certaines de ces pièces jointes contiennent des informations sur des personnes, des sociétés ou des autorités en lien notamment avec des procédures d'entraide judiciaire en matière pénale.

121 La pièce jointe « [redacted].doc » contient une capture d'écran de la page de garde d'une décision de la Cour des plaintes du Tribunal pénal fédéral du

[65] AUD 03.10.01.1.
[66] B03.10.01.01.
[67] B03.10.01.02.
[68] B03.10.01.03.
[69] B03.10.01.04.
[70] B03.10.01.05.
[71] B03.10.01.06.
[72] B03.10.01.07.
[73] B03.10.01.08.
[74] B03.10.01.09.
[75] B03.10.01.10.
[76] B03.10.01.11.
[77] B03.10.01.12.
[78] B03.10.01.13.
[79] B03.10.01.14.

22 février 2007, rendue dans le cadre d'une procédure d'entraide internationale en matière pénale. Les noms des parties ne sont ni caviardés, ni anonymisés. L'adresse du recourant est également indiquée.

122 La pièce jointe « [redacted]*.docx* » est un document qui contient des captures d'écran de l'application PAGIRUS, dans lesquelles des raisons sociales de personnes morales dont les avoirs ont été séquestrés ou restitués sont visibles.

6. Cas de transfert actif n° 2 : un tableur Excel concernant 156 patrouilles de la Police militaire (30 juillet 2020)

123 Le contexte est le suivant : un employé de la Police militaire (« H ») envoie un e-mail intitulé « [redacted] », le 29 juillet 2020 à 13h40, depuis l'adresse [H]@vtg.admin.ch, à un employé de la BAC (« I »), sur son adresse [I]@vtg.admin.ch[80].

124 En substance, H indique qu'il doit ajouter 156 nouvelles patrouilles dans l'application JORASYS, mais que cette opération nécessite beaucoup de temps, raison pour laquelle il a besoin d'aide :

> «*Ich muss 156 neue Patrouillen im JORASYS-System anlegen.*
>
> *Aber diese Operation nimmt viel Zeit in Anspruch. Deshalb komme ich zu Ihnen, um zu sehen, ob es möglich ist, die derzeitige Liste "1970 Patrouillennummer" durch diese neue, von mir erstellte Liste zu ersetzen.* »

125 Cet e-mail figure dans des e-mails subséquents et le texte qu'il contenait est ainsi visible. Il n'y a pas d'indice que son texte ait été modifié dans les échanges subséquents. En revanche, l'e-mail original ne figure pas parmi les données à notre disposition.

126 Moins de dix minutes plus tard (29 juillet 2020, 13h49), I répond à H par e-mail non chiffré en lui demandant d'ouvrir un « *Incident* » auprès de la *Hotline* de la BAC, afin que I puisse le transmettre « au prestataire »[81] :

> « *Guten Tag [***] [nom de H]*
>
> *Damit ich das dem Lieferanten zustellen kann, benötige ich einen Incident. Können Sie bitte einen Incident bei ser FUB Hotline eröffnen lassen.* »

127 Environ deux heures plus tard (29 juillet 2020, 15h44), H envoie un e-mail depuis son adresse [H]@vtg.admin.ch au Service Desk de la BAC, avec copie à I[82].

128 En substance, H demande au Service Desk de la BAC d'ouvrir un incident et de transmettre ce dernier à : « *bitte öffnen Sie einen Vorfall und leiten Sie ihn an [nom/prénom de I] (*[I]*@vtg.admin.ch) weiter*. »

129 Cet e-mail figure dans des e-mails subséquents et le texte qu'il contenait est ainsi visible. Il n'y a pas d'indice que son texte ait été modifié dans les échanges subséquents. En revanche, l'e-mail original ne figure pas parmi les données à notre disposition.

130 Le lendemain (30 juillet 2020, 7h50), I transfère par e-mail non chiffré l'e-mail intitulé « [redacted] » à un employé de Xplain (« U »), à son adresse [U]@xplain.ch, ainsi qu'à l'adresse support@xplain.ch[83]. H est en copie.

131 En substance, I indique ce qui suit :

---

[80] AUD 03.10.05.1-4.
[81] AUD 03.10.05.1-4.
[82] AUD 03.10.05.5-8.
[83] AUD 03.10.05.5-8.

« Guten Tag Herr [nom de U]

Können Sie das bitte anschauen.

[redacted]

Beste Grüsse

[prénom nom de I] »

132 Cet e-mail contient une pièce jointe intitulée « [redacted] *.xls* »[84]. Il s'agit d'un tableur Excel (.xls) comptant 264 lignes et une dizaine de colonnes. Ces lignes et colonnes contiennent visiblement des données relatives aux 156 patrouilles de la Police militaire évoquées par H dans ses e-mails précités. Ce tableur mentionne tout ou partie des éléments suivants :

- Prénom et nom des personnes physiques,
- Numéro de téléphone portable,
- Lieu d'affectation,
- Lieu d'entrée en service.

133 Environ une heure plus tard (30 juillet 2020, 9h29), Q envoie un e-mail non chiffré à I depuis l'adresse support@xplain.ch. Q indique ce qui suit[85] :

«Guten Tag,

in der Beilage finden Sie das DB-Script, das die neuen Patrouillen einfügt und die alten inaktiv setzt.

Darf ich Sie bitten, dieses Script zuerst auf der Test- und dann auf der Produktionsumgebung ausführen zu lassen.

Freundliche Grüsse

[Q].»

134 L'e-mail non chiffré de Q contient en pièce jointe un fichier intitulé « [redacted] sql »[86]. Ce fichier contient notamment les informations relatives aux nouvelles patrouilles de la Police militaire issues du tableur Excel susmentionné (notamment prénom, nom, numéro de téléphone portable).

135 Enfin, le même jour (30 juillet 2020), à 15h52, I informe H par e-mail de ce qui suit, avec copie à U et à l'adresse support@xplain.ch : « *Wir haben das erfolgreich auf die Produktion gespielt*. »

7. Cas de transfert actif n° 3 : la capture d'écran d'un extrait d'une audition (12 janvier 2018)

136 Le contexte est le suivant : un employé de fedpol adresse, depuis son adresse @fedpol.admin.ch, un e-mail non chiffré le 11 janvier 2018 à 11h37 au Service Desk du système JANUS (bkpjanushelp@fedpol.admin.ch), en demandant de régler un problème d'affichage et de formatage des documents générés dans ORMA[87] :

[84] AUD B03.10.05.01.
[85] AUD 03.10.05.9-12.
[86] AUD B03.10.05.03.
[87] AUD 03.10.02.21.

« Beim Erstellen eines Berichtes, bzw. beim einfügen des Sachverhaltes wurde festgestellt, dass sich die Nummern der Untertitel in der Formatvorlage nicht auf den dazugehörenden Haupttitel beziehen. Der Nummerierungswert kann auch nicht neu festgelegt werden, da diese Funktion nicht aktiviert ist.

Des Weiteren ist die ganze Formatvorlage in einer 1er-Zeilenschaltung definiert. Gemäss gängiger Rapportlehre sollte der ganze Sachverhalt in 1.5-Zeilenschaltung erstellt werden. »

137 Cet e-mail contient notamment une capture d'écran d'un procès-verbal d'une audition apparemment menée par fedpol. Le nom et le prénom de la personne entendue sont visibles de même que ses déclarations (non verbatim).

138 Cet e-mail figure dans des e-mails subséquents et le texte et les captures d'écran qu'il contenait sont ainsi visibles. Il n'y a pas d'indice que son contenu ait été modifié dans les échanges subséquents. En revanche, l'e-mail original ne figure pas parmi les données à notre disposition.

139 Environ sept heures plus tard (11 janvier 2018, 18h21), un employé du Service Desk « Janus » transfère cet e-mail, depuis l'adresse bkpjanushelp@fedpol.admin.ch, par e-mail non chiffré à deux collaborateurs de fedpol.

140 Ces collaborateurs sont d'une part F et d'autre part S, qui était employé de Xplain en 2010[88] mais était employé de fedpol en 2018. Selon l'information reçue de fedpol, les rapports de travail entre fedpol et S ont débuté le 1er décembre 2015[89].

141 L'employé du Service Desk « Janus » indique ce qui suit :

« Könntet ihr bitten den Vorschlag von Herrn [nom de l'utilisateur fedpol], prüfen? Das Problem mit der Formatvorlagen kommt auch bei mir vor.

Ich konnte leider nicht herausfinden, wie man die Anzeigeprobleme lösen kann. Wisst ihr wo das Problem liegt? » [90]

142 Le lendemain (12 janvier 2018, 11h56), F transfère depuis son adresse [F]@fedpol.admin.ch les deux e-mails précités du 11 janvier 2018, par e-mail non chiffré intitulé « [redacted] *(*» à T à son adresse [T]@xplain.ch. S est en copie.

143 Dans cet e-mail, F évoque les problèmes d'affichage des documents générés dans ORMA et sollicite son assistance[91] :

« Hallo [prénom de T]

Da haben wir trotzt Fix noch ein Problem mit der Formatvorlage. Jede Überschrift muss nochmals eingestellt werden mittels der Wordfunktion.
Siehe Bild 1 welches ich erstellt habe und jenes von den User die es bemängelt haben.
Desweiteren sind die Abstände nicht in Ordnung mit einer Überschrift 2 beispielsweise.

Schaue es Dir nochmals an und sag uns was hierfür gemacht werden kann. »

144 Le même jour (12 janvier 2018, 15h37), T répond à F par e-mail non chiffré, avec S est en copie[92] :

---

[88] Cf. *supra* par. 107, ainsi que AUD B03.04.10.237; AUD B03.04.10.208.
[89] AUD B03.04.10.715.
[90] AUD 03.10.02.21.
[91] AUD 03.10.02.26.
[92] AUD 03.10.02.33.

« Hallo [prénom de F]

Ich schaue dies mit diesem Focus an. (…) »

8. Cas de transfert actif n° 4 : une vidéo transmise dans le cadre d'une demande de support, révélant des noms et adresses de prévenus, témoins, avocats et enquêteurs d'une procédure pénale (12 décembre 2014)

145 Le contexte est le suivant : à fin 2014, il semble que des enquêteurs de fedpol aient constaté des lenteurs et rencontré des problèmes lors de l'utilisation de ORMA[93]. L'application était affectée en particulier dans sa fonctionnalité hors réseau (« *offline Funktionalität* »)[94].

146 Le 17 décembre 2014, F adresse un e-mail à S ([S]@xplain.ch) et un administrateur de Xplain (« V ») ([V]@xplain.ch) où il indique notamment :

> *« Die grösste Problematik stellt die „offline Funktionalität". Die Ermittler haben mit ORMA zur Zeit kein stabiles offline Tool mehr, um ihre Hausdurchsuchungen und externe offline Einvernahmen zu bewerkstelligen!*
>
> *(…)*
>
> *Die derzeitige Situation ist wirklich sehr unglücklich und ernst zu nehmen! »*[95].

147 Le cas décrit ici s'inscrit dans le contexte des travaux menés par fedpol et Xplain pour remédier à ces problèmes.

148 Le 12 décembre 2014 à 13h21, F envoie un e-mail non chiffré intitulé « [redacted] » à S, à son adresse [S]@xplain.ch[96] :

> « *Tschou [surnom de S]*
>
> *Schau mal folgende Problematik mit den WinWord Instanzen. Meinst Du das wir solches auch in den Griff bekommen? Insgesamt sind 3 Dokumente geöffnet und es kann nicht richtig gesteuert werden.*
>
> *LG*
>
> *[prénom de F]*
>
> *Von meinem iPhone gesendet* ».

149 L'e-mail contient une pièce jointe intitulée « [redacted]*.zip* ». Ce fichier compressé (.zip) contient à son tour un fichier « [redacted]*.MP4* »[97]. En substance, il s'agit d'un enregistrement vidéo en format .MP4 de 71 secondes, lequel reproduit une assistance informatique à distance (« *Windows Remoteunterstützung* ») fournie à un enquêteur fedpol.

[93] AUD 03.10.02.10-11.
[94] AUD 03.10.02.10-11.
[95] AUD 03.10.02.10-11.
[96] AUD 03.10.02.8.
[97] AUD B03.10.02.09.

150 A compter de la seconde 00:29 de l'enregistrement, le procès-verbal d'une audition de témoin déléguée à fedpol par le Ministère public de la Confédération dans le cadre d'une procédure pénale est visible à l'écran. Les éléments suivants sont visibles :

- Nom et prénom(s) du témoin ;
- Date et lieu de naissance du témoin ;
- Nationalité du témoin ;
- Permis de séjour et validité de ce dernier ;
- Langue du témoin ;
- Nom des parents du témoin ;
- Etat-civil – nom et prénom du conjoint ;
- Profession du témoin ;
- Adresse de domicile du témoin ;
- Date, lieu et heure de l'audition ;
- N° de la procédure pénale ;
- Nom et prénom des prévenus, avec les infractions soupçonnées pour chacun d'eux ;
- Nom et prénom(s)de l'enquêteur et du rédacteur du procès-verbal ;
- Mention que l'interprète est connu(e) de la Police judiciaire fédérale ;
- Nom et prénom(s) d'avocats.

151 Quelques semaines plus tard, le 6 janvier 2015 à 11h34, l'enquêteur qui avait reçu l'assistance à distance enregistrée dans la vidéo précitée, constate de nouveaux problèmes affectant ORMA et s'adresse par e-mail à un autre employé de fedpol (« J »)[98].

152 Cet e-mail figure dans des e-mails subséquents et le texte et les captures d'écran qu'il contenait sont ainsi visibles. Il n'y a pas d'indice que son contenu ait été modifié dans les échanges subséquents. En revanche, l'e-mail original ne figure pas parmi les données à notre disposition.

153 Environ quinze minutes plus tard (6 janvier 2015, à 11h50), J transfère l'e-mail précité de l'enquêteur, par e-mail non chiffré intitulé « [redacted] !!! », à l'adresse support@xplain.ch, avec copie à F :

> *« Hallo zäme*
>
> *Ich wünsche euch allen ein erfolgreiches und glückliches 2015!*
>
> *Leider gibt's auch in diesem Jahr wieder Supportanfragen – hier hat [prénom de l'enquêteur] Probleme mit ORMA, die sogar sein Programm beenden.*
>
> *Habt Ihr eine Idee, woran das liegen könnte?*
>
> *Vielen Dank für eure Bemühungen »*[99].

154 L'e-mail transféré à Xplain par J contient quatre captures d'écran, sur lesquels sont visibles une partie de la première page d'un rapport de fedpol relatif à l'audition du témoin dont le procès-verbal était visible

[98] AUD 03.10.02.13-17.
[99] AUD 03.10.02.13.

dans la vidéo précitée, ainsi qu'une partie de la première page d'un autre rapport de fedpol. Le premier rapport cité indique que le témoin en question a remis deux DVD dans le cadre de son audition. Les informations suivantes sont également visibles :

- Nom du témoin ;
- Date de naissance du témoin ;
- Nationalité du témoin ;
- Nom des parents du témoin ;
- Etat-civil – nom et prénom du conjoint ;
- Date et lieu de l'audition.

155 Ces informations sont identiques à celles visibles sur l'enregistrement vidéo précité.

9. Cas de transfert « semi-automatique » : la fonctionnalité « *Error Reporting* »

a) Description générale

156 Selon les constatations de l'Organe d'enquête, la fonctionnalité dite de « *Error Reporting* » (ou « *Fehlermeldung* ») permettait d'enregistrer une erreur survenue dans une application, afin qu'elle puisse être analysée et traitée. Xplain l'a intégrée dans différentes applications qu'elle a développées. Le but poursuivi par Xplain était apparemment de faciliter les prestations de support aux utilisateurs[100].

157 La fonctionnalité a été identifiée à tout le moins au sein des applications suivantes : ORMA (fedpol), TROVA (OFJ), eneXs (OFDF) et JORASYS (PM et BAC)[101].

158 Des indications suggèrent que la fonctionnalité a été intégrée dans ORMA en tout cas dès 2019, voire en septembre 2017[102]. Un manuel daté de juillet 2017 à l'en-tête de Xplain suggère que la fonctionnalité de *Error Reporting* existait alors dans TROVA[103]. L'introduction semble avoir eu lieu en 2015[104] déjà au sein de eneXs. S'agissant de JORASYS, il apparaît que la fonctionnalité était présente à tout le moins dès 2020[105]. En définitive, la date exacte de l'introduction de cette fonctionnalité dans les applications fournies par Xplain n'a pas pu être identifiée de manière certaine. Il semble en toute hypothèse que la fonctionnalité n'ait pas été intégrée dans les applications précitées au même moment.

159 En substance, le processus de « *Error Reporting* » se présentait de la manière suivante[106] :

- Un utilisateur constate la survenance d'une erreur en cours d'utilisation d'une application ;
- Il active la fonctionnalité de « *Error Reporting* » en appuyant sur une case ou une touche prévue à cet effet dans l'application concernée ;
- L'utilisateur reproduit l'erreur qu'il a constatée, de sorte à ce que la fonctionnalité puisse effectuer en arrière-plan les démarches suivantes :
    - Prise de captures d'écran de tous les moniteurs connectés (une image par seconde) ;

[100] AUD 03.10.08.48.
[101] AUD 03.10.10.1-200.
[102] AUD 03.10.10.135-201.
[103] AUD 03.10.10.202-231.
[104] AUD 03.10.10.130-134.
[105] AUD 03.10.10.46-129.
[106] AUD 03.04.02.11 ; AUD 03.06.01.17 ; B03.06.01.07 ; AUD 03.10.10.1-200.

- Préparation d'un protocole et de fichiers journaux (notamment des données logs) ;
- Si nécessaire, « réalisation de diagnostics fonctionnels spécifiques »[107] ;

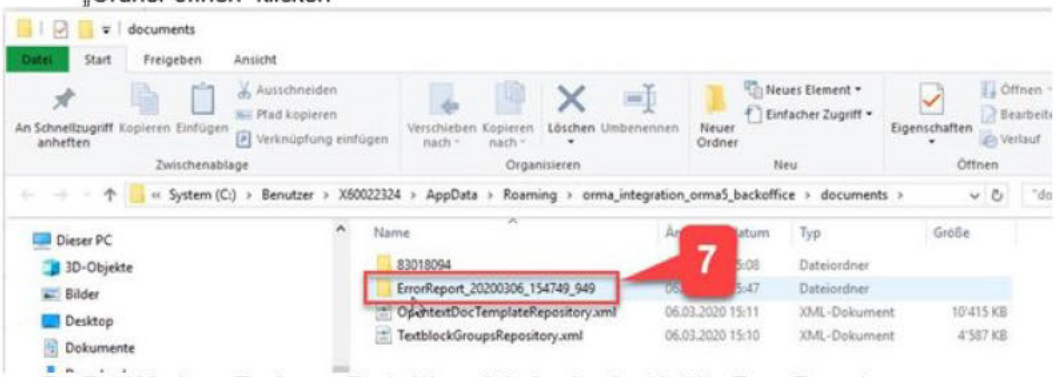
- L'utilisateur met fin à la procédure d'enregistrement en appuyant sur une case ou une touche prévue à cet effet ;
- Un fichier .ZIP (en règle générale dénommé « [redacted]*[xxx].zip* »), dans lequel se trouvent toutes les captures d'écran ainsi que les fichiers journaux (notamment données logs), est automatiquement créé ;
- L'utilisateur obtient confirmation de l'enregistrement et peut accéder au fichier .ZIP sauvegardé.

160 Afin que l'erreur puisse être traitée par les personnes en charge du support interne, le fichier [redacted]*xxx].zip* » doit leur être transmis par l'utilisateur. Dans plusieurs cas, nous avons constaté que le fichier .zip était ensuite transmis à Xplain par le support interne. Les canaux de transmission identifiés sont les suivants :

- Envoi en tant que pièce jointe par e-mail[108] ;
- Envoi en tant que pièce jointe par le biais de l'application JIRA (système de « *tickets* ») ;
- Mise à disposition du fichier sur la plateforme WebFTP de l'OFIT[109] ; ou
- Dépôt du fichier sur le disque réseau (T:) de l'unité concernée (« *T-Laufwerk* »)[110].

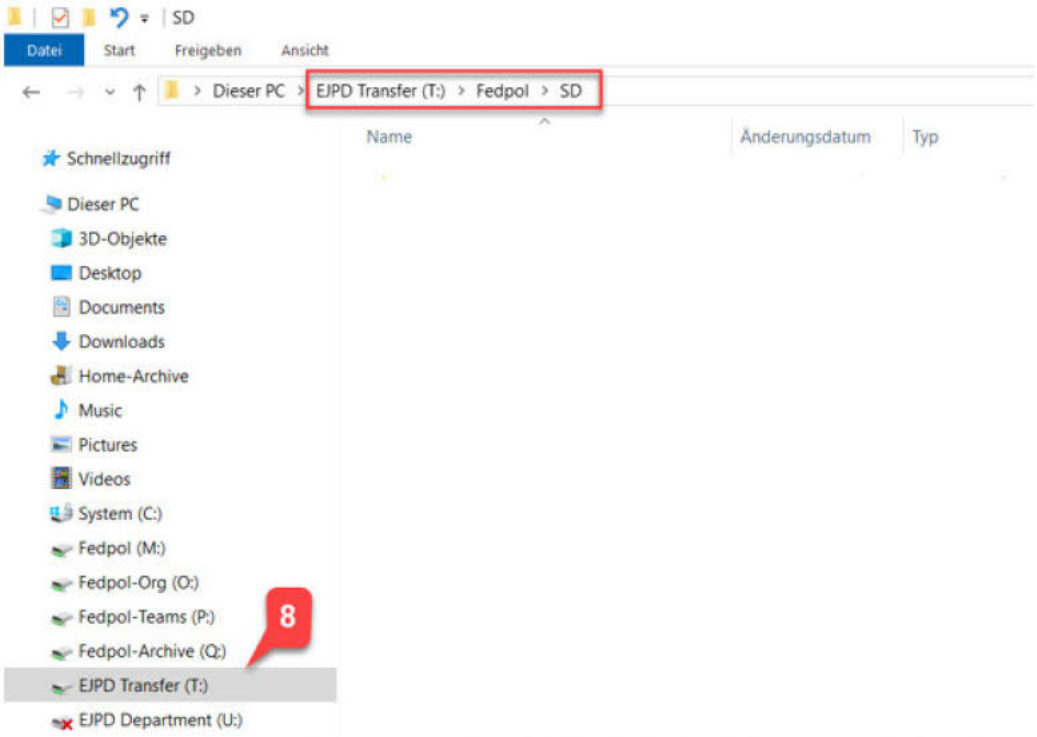
161 A titre illustratif, le *Handbuch Service Desk ORMA* du 23 octobre 2020 (version 1.2), sur papier en-tête de fedpol (« Service Desk & Digitale Ausbildung ») et portant la mention « divers auteurs » (« *Autoren verschiedene* »), se présentait comme suit (extrait) :

6. Ein Fenster öffnet sich und bestätigt, dass der Error Report erstellt wurde. Nun auf „Ordner öffnen" klicken



7. Der Windows Explorer öffnet sich und darin abgelegt ist der Error Report.

[107] L'expression est utilisée dans un manuel d'utilisation, mais sa portée exacte n'est pas claire.
[108] Cela représente alors, selon les hypothèses de travail retenues dans cette enquête, un « transfert actif » ou un « *forward* ».
[109] Voir par exemple : e-mail envoyé à [R]@xplain.ch depuis l'adresse webftp@bit.admin.ch le 15 juin 2017, à 15h12, intitulé « *Word Dokumente im TROVA (www.webftp.admin.ch)* » (AUD 03.10.10.241-244).
[110] AUD 03.06.01.17.



8. File auf dem Transfer-Laufwerk ablegen. Anschliessend Abnahme durch das Service Desk

162 Cette fonctionnalité pourrait être qualifiée de « semi-automatique ».

163 D'un côté, elle suppose nécessairement une intervention manuelle de l'utilisateur afin d'activer la fonctionnalité et de transmettre le fichier .ZIP aux personnes en charge du support interne. Pour parvenir dans l'environnement informatique de Xplain, ces données doivent ensuite être transmises ou mises à disposition de Xplain.

164 D'un autre, l'enregistrement des activités à l'écran (sur tous les moniteurs) et la création des autres données (en particulier fichiers journaux), ainsi que la création du fichier .ZIP, interviennent de manière automatisée. Par ailleurs, il a été constaté que des fichiers « [redacted]*[xxx].zip* » contiennent parfois d'autres fichiers que les captures d'écran ou les fichiers journaux. Selon les constations faites par l'OFJ en mai 2020, à la fin de l'enregistrement opéré par la fonction *Error Reporting* dans l'application TROVA, l'ensemble du répertoire temporaire de l'application était automatiquement compressé dans un fichier .ZIP[111].

165 OA a identifié plusieurs manuels d'utilisateur (« *Benutzerhandbücher* ») relatifs aux applications fournies par Xplain. Ces manuels d'utilisateur, généralement sur papier en-tête de Xplain, décrivent de manière plus ou moins détaillée le fonctionnement de cette fonctionnalité « *Error Reporting* ».

166 La plupart de ces manuels se limitent à indiquer que tout ce qui est affiché à l'écran est enregistré pendant le processus : « *es wird der gesamte Bildschirm dahinter aufgezeichnet* ». Tel est par exemple le

[111] AUD B12.02.01.38 et 40.

cas du manuel d'utilisation de l'application TROVA précité daté d'août 2017[112]. S'agissant de l'application ORMA, un « *ORMA Handbuch Service Desk* » daté de mars 2021 énumère les étapes du processus de « *Error Reporting* », sans contenir la précision précitée[113].

167 Toutefois, deux manuels contiennent une précision qui n'est présente dans aucun des autres manuels identifiés par OA (mise en évidence conforme à l'original) :

> ***ATTENTION : Pendant l'enregistrement des rapports d'erreur, des captures d'écran sont faites de tous les moniteurs connectés. Pour des raisons de protection des données, veuillez fermer toutes les fenêtres contenant des informations sensibles***[114].

168 Le premier manuel concerne apparemment eneXs 2.6.2. A l'en-tête de Xplain, il date du 28 février 2020 dans sa version allemande. Le passage cité ci-dessus est issu d'une traduction d'une partie du manuel (4 pages), laquelle date apparemment du 29 juillet 2021.

169 Le premier manuel se trouvait dans la boîte e-mail d'un employé du SRC en date du 29 juillet 2021, qui l'a reçu de Xplain. Cet envoi par Xplain fait suite à une demande cet employé du SRC d'obtenir une traduction en français dans le but suivant : « *Haben Sie dies Anleitung auch auf französisch? Dann kann ich die Mitarbeiter PSI in Genf informieren.* »[115]

170 Le second manuel concerne apparemment JORASYS 0.9.4. A l'en-tête de Xplain, il date d'avril 2022 et compte 83 pages en allemand. En page 79, il contient une précision analogue à celle citée plus haut.

171 Le second manuel se trouvait dans la boîte e-mail d'un employé de la Police militaire en date du 26 avril 2022, avec deux autres fichiers .pdf reçus de Xplain à la même occasion. Dans son e-mail d'accompagnement, l'employé de Xplain, germanophone, indique à cet employé de la Police militaire, francophone[116] :

> *Ces documents nous allons besoins le 31.05.2022. La semaine prochaine nous pouvons discuter quoi nous allons faire le 31.05.2022. Pour cette discussion je te demande de lire les deux PDF annexés. Le « Benutzerhandbuch » tu n'as pas besoin de lire, parce que c'est mieux de l'utiliser avec l'application.*

172 L'Organe d'enquête n'a pas identifié de plus amples informations qui permettraient de tirer des conclusions sur la diffusion éventuelle de ces deux manuels par les personnes qui les ont reçues.

173 L'enquête a en outre révélé que, en mai 2020, un employé de l'OFJ (« L ») a identifié des risques liés à la fonctionnalité de « *Error Reporting* ». Dans un e-mail intitulé « *Übermittlung von Inhalten in den TROVA ErrorReports* » adressé le 7 mai 2020 à un employé de Xplain, avec copie à un autre employé de l'OFJ, il indique notamment que :

> *« Dabei ist mir aufgefallen, dass bei der Aufzeichnung geöffnete Inhalte (PDF, WORD etc.) pauschal im Report enthalten sind bzw. damit aus TROVA exportiert werden. Dies ist aus datenschutzrechtlichen Gründen und insbesondere aufgrund der sensiblen Daten in TROVA höchst fragwürdigst und schwer zu rechtfertigen.*
>
> *(…)*

[112] AUD 03.10.10.41.
[113] AUD 03.10.10.201.
[114] AUD 03.10.10.132.
[115] AUD 03.10.232-237.
[116] AUD 03.10.10.238-240.

Werde das in JIRA als Verbesserung für das Produkt eingeben, bis dahin können wir als Umgehungslösung ggf. die Inhalte aus dem Report löschen. »[117]

174 Deux mois plus tard, en juillet 2020, L a ouvert un ticket sur la plateforme JIRA intitulé « *Fehlerbericht aufzeichnen : opt-in für Export von Inhalten* ». Le ticket porte sur une demande d'amélioration (« *Verbesserung* ») à apporter à TROVA et il est résumé comme suit :

« Als Benutzer/in von TROVA kann ich beim Erstellen einer Fehlermeldung selbst entscheiden, ob Inhalte, die beim Aufzeichnen des fehlerhaften Anwendungsfalls "betroffen" sind, zusammen mit den weiteren, notwendigen Inhalten/Daten (wie z. B. das Application Log aus dem %appdata%-Verzeichnis) exportiert werden, um die Anforderungen an den Datenschutz besser steuern zu können und die Inhalte nicht im Anschluss nach dem Export einzeln oder überhaupt aus dem ZIP entfernen zu müssen »[118].

175 Par la suite un collaborateur de l'OFJ, dont le nom n'est pas précisé dans le document à notre disposition, a indiqué à Xplain que cette amélioration souhaitée par l'OFJ pourrait vraisemblablement intéresser ou être pertinente pour d'autres clients de Xplain (« *Vorstellen könnte ich mir hier, dass dies auch für andere Kunden interessant/relevant sein könnte?* »)[119].

176 Selon les données à notre disposition, Xplain a fait preuve de réticence face à l'amélioration demandée. En septembre 2020, un employé de Xplain a indiqué par e-mail : « *Das Opt-Out für den Error-Report werden wir nicht umsetzen, da dies aus unserer Sicht keinen Sinn macht. Der Inhalt des Error Reports hilft uns Fehler zu klären. Es gäbe aber die Möglichkeit den Error Report zu deaktivieren, falls er zu Problemen beim Datenschutz führt* »[120].

177 Après avoir finalement reçu de Xplain en mars 2021 une estimation selon laquelle le changement demandé représenterait 80h de travail, il semblerait que l'OFJ ait provisoirement renoncé à sa demande d'amélioration de TROVA. En juin 2021, Xplain et l'OFJ se sont apparemment entendus pour que l'amélioration en question soit intégrée lors du passage de la version 1.7 à la version 2.0, ce qui ne semble en définitive pas avoir été fait. Cependant, nonobstant le maintien de cette fonctionnalité dans TROVA, et d'après l'interrogatoire d'un employé de l'OFJ, les utilisateurs de TROVA auraient reçu de l'OFJ des consignes d'utilisation de cette fonctionnalité de « *Error Reporting* »[121].

178 Au terme de l'enquête, il ne semble pas que l'OFJ ait informé d'autres unités administratives de la Confédération des risques que présentait la fonctionnalité de « *Error Reporting* », selon sa propre analyse, sous l'angle de la protection des données.

179 Comme indiqué plus haut, OA a signalé à l'Organe de coordination par e-mail chiffré du 1er décembre 2023 l'existence de cette fonctionnalité. Selon l'information reçue de l'Organe de coordination, cette fonctionnalité a été désactivée en été 2023. Les directives internes ont été adaptées et les produits (*software*) concernés sont en cours de mise à jour afin de supprimer définitivement la fonctionnalité.

[117] AUD 03.10.08.1-3.
[118] AUD 03.10.08.7.
[119] AUD 03.10.08.49.
[120] AUD 03.10.08.48.
[121] AUD 03.10.08.49.

b) Exemple : envoi de captures d'écran de pièces d'identité

180 Un employé de l'OFDF (« M ») envoie un e-mail non chiffré le 24 octobre 2016 à 10h21, depuis son adresse [M]@bazg.admin.ch, intitulé « [redacted] », à un employé de Xplain (« Y »), à son adresse [Y]@xplain.ch. Un autre employé de l'OFDF se trouve en copie[122].

181 Dans cet e-mail, M indique à Y qu'il n'a pas pu le joindre par téléphone et que ZEMIS ne fonctionne pas correctement. A demande également à X de le rappeler dès que possible :

> *« Hallo [surnom de Y].*
>
> *Konnte dich telefonisch nicht erreichen.*
>
> *Wir haben Probleme mit ZEMIS. Die Verteilung der 1.8.1.0 ist letzte Woche (am 18.10.16) erfolgt. Irgendwas stimmt aber nicht. Bin gerade etwas ratlos.*
>
> *Kannst du mich anrufen sobald du Zeit hast?*
>
> *Merci und Gruss*
>
> *[surnom de M] »*

182 ZEMIS est l'abréviation de *Zentrale Migrationsinformationssystem* (système d'information central sur la migration SYMIC)[123].

183 Cet e-mail contient une pièce jointe intitulée « [redacted]*zip* ». Ce fichier compressé représente environ 21 Mo. Il contient des captures d'écran de pièces d'identités de personnes. En substance, le nom, le prénom, la nationalité et, dans un cas la photo d'identité, des personnes en question sont visibles.

184 Moins de cinq minutes plus tard (24 octobre 2016, 10h25) M envoie un autre e-mail à Y, à son adresse [Y]@xplain.ch, sans pièce jointe. Le texte est identique au premier e-mail, à l'exception de la phrase suivante qui a été ajoutée :[124]

> *« Habe dir das Error Zip und eine eneXs2 Version welche das Problem hat auf das Transfer LW gelegt. T:\EFD\EZV\GWK ZEMIS. »*

185 « LW » ne peut signifier que « *Laufwerk* » dans ce contexte. En d'autres termes, M a sauvegardé le fichier compressé [redacted].zip précité sur un disque réseau de la Confédération, à l'attention de Y.

186 Le fait que M envoie d'abord à 10h21 un e-mail à Y à son adresse [Y]@xplain.ch contenant un fichier .zip d'environ 21 Mo, puis que M, à 10h25, mette à disposition de Y le même fichier .zip sur le serveur T: de la Confédération, soulève la question de savoir si Y a reçu l'e-mail de 10h21 ou s'il ne lui a pas été remis (par exemple en raison de la taille de la pièce jointe). Dans les données à notre disposition, nous n'avons pas identifié de message d'erreur indiquant que cet e-mail n'a pas été remis, mais nous n'avons pas non plus identifié de réponse à l'e-mail de 10h21.

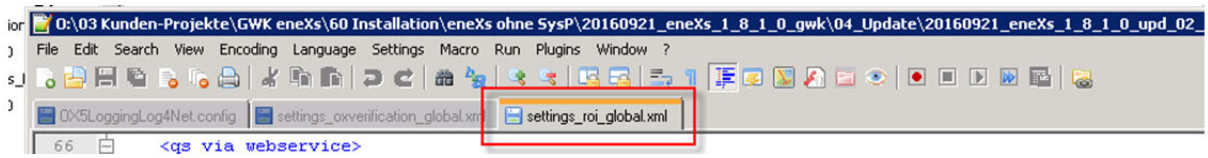
187 En revanche, une réponse de Y au second e-mail de M envoyé à 10h25 a été identifiée.

188 Dans un e-mail non chiffré envoyé depuis l'adresse [Y]@xplain.ch le même jour (24 octobre 2016, 14h39), Y transmet à M un fichier [redacted].xml contenant du code et lui demande de vérifier un point[125] :

---

[122] AUD 03.10.07.1.
[123] RS 142.513.
[124] AUD 03.10.07.4.
[125] AUD 03.10.07.7.

Kannst du bitte prüfen ob dort bei dir nach der Verteilung folgendes drin steht:



189 La signature automatique suivante figure au pied de l'e-mail envoyé par Y depuis son adresse [Y]@xplain.ch :

Freundliche Grüsse
Y

deXplain GmbH
Y
Ring 38
D-04416 Markkleeberg
+49
Y @xplain.ch
www.xplain.ch

190 Moins de trente minutes plus tard (24 octobre 2016, 15h04), M répond à Y par e-mail non chiffré en lui informant que le problème a été résolu : « *Habe den Fehler gefunden* »[126].

10. Le fichier .xml (septembre 2015) qui comprend certaines données du système d'information HOOGAN, dont l'existence a été médiatisée (canal inconnu)

191 Le *Datendump* contient un fichier intitulé « *xml* » daté du 4 septembre 2015. Ce fichier inclut des extraits du système d'information HOOGAN géré par fedpol.

192 L'enquête n'a pas permis de clarifier les circonstances factuelles dans lesquelles ce fichier s'est trouvé dans l'environnement informatique de Xplain.

11. Le tableur Excel contenant des données des utilisateurs de JORASYS au sein de la Police militaire, dont l'existence a été médiatisée (canal inconnu)

193 Le *Datendump* contient un fichier intitulé « *xlsx* » daté du 18 septembre 2020. Ce fichier compte 718 lignes de données relatives à des utilisateurs de JORASYS au sein de la Police militaire.

194 L'enquête n'a pas permis de clarifier les circonstances factuelles dans lesquelles ce fichier s'est trouvé dans l'environnement informatique de Xplain.

B. Relations avec Xplain

1. Entrée en relation

195 L'ancienneté des faits rend difficile la clarification de l'origine des relations entre la Confédération et Xplain. Ainsi, la majorité des personnes interrogées ont indiqué ignorer quand et comment leur unité administrative est entrée en relation avec la société Xplain. De même, les pièces remises par les Unités

[126] AUD 03.10.07.7.

touchées et les données électroniques à disposition de l'Organe d'enquête ne contiennent que peu d'informations sur les années antérieures à 2005.

196 Il ressort toutefois de certains interrogatoires, ainsi que des contrats et de certaines Données Exchange, que l'origine des relations entre la Confédération et Xplain se situe en 2001-2002.

197 A cette époque, les deux fondateurs de Xplain, qui nous ont été décrits comme d'anciens collaborateurs de la société rola Security Solutions GmbH, dont le siège est en Allemagne, ont obtenu un contrat avec le Corps des gardes-frontière (« Cgfr »). Le contrat s'inscrivait dans le cadre du projet « *Rumaca* » du Cgfr[127]. Xplain n'avait pas pour tâche de développer un logiciel – cette tâche revenait à la société UNISYS – mais de conseiller le Cgfr dans le cadre du projet.

198 Entre 2000 et 2003, Xplain a apparemment fourni deux produits à fedpol (doXstore et noteboX). Un e-mail interne à fedpol de 2010 montre que les collaborateurs de fedpol rencontraient des difficultés à identifier la documentation relative à l'attribution à Xplain de ces mandats[128].

199 En annexe à l'e-mail en question figure un document de quatre pages du 29 avril 2003 intitulé « *Argumentarium für Ausnahmegenehmigung EJPD-GEVER-STRATEGIE* » à l'en-tête de fedpol (alors « fedpol.ch »). Ce document, dont l'auteur n'est pas identifié, indique que la Police judiciaire fédérale (PJF) prévoit la mise en œuvre de l'application « ORMA » en 2004 en tant qu'outil de gestion des affaires et dossiers (« *Geschäfts- und Dossierverwaltung* »).

200 Ce document expose qu'une « comparaison détaillée » du produit « FABASOFT » (de la société du même nom) et du produit « worX » (de la société Xplain) a conduit au constat que seul le produit d'Xplain rempli les exigences posées. L'enquête n'a pas permis de localiser cette « comparaison détaillée ».

201 Le document indique ensuite au point 5 :

5 Zusammenfassung / Vorgaben / Bedingungen

- Termin, Geschäfts- und Dossierverwaltung muss bei Beginn der Dezentralisierung im Februar 2004 voll einsatzfähig sein.
- Die Geschäfts- und Dossierverwaltung muss durchgängig zu bestehenden Systemen wie Rapportsystem, Journal, und Janus+ PV sein. Zudem muss eine Schnittstelle zu IPAS realisiert werden.
- Die Vorschläge von PPS sind zu berücksichtigen.
- Die Lösung soll kostengünstig und flexibel sein, sowie keine präjudizierende Wirkung haben.

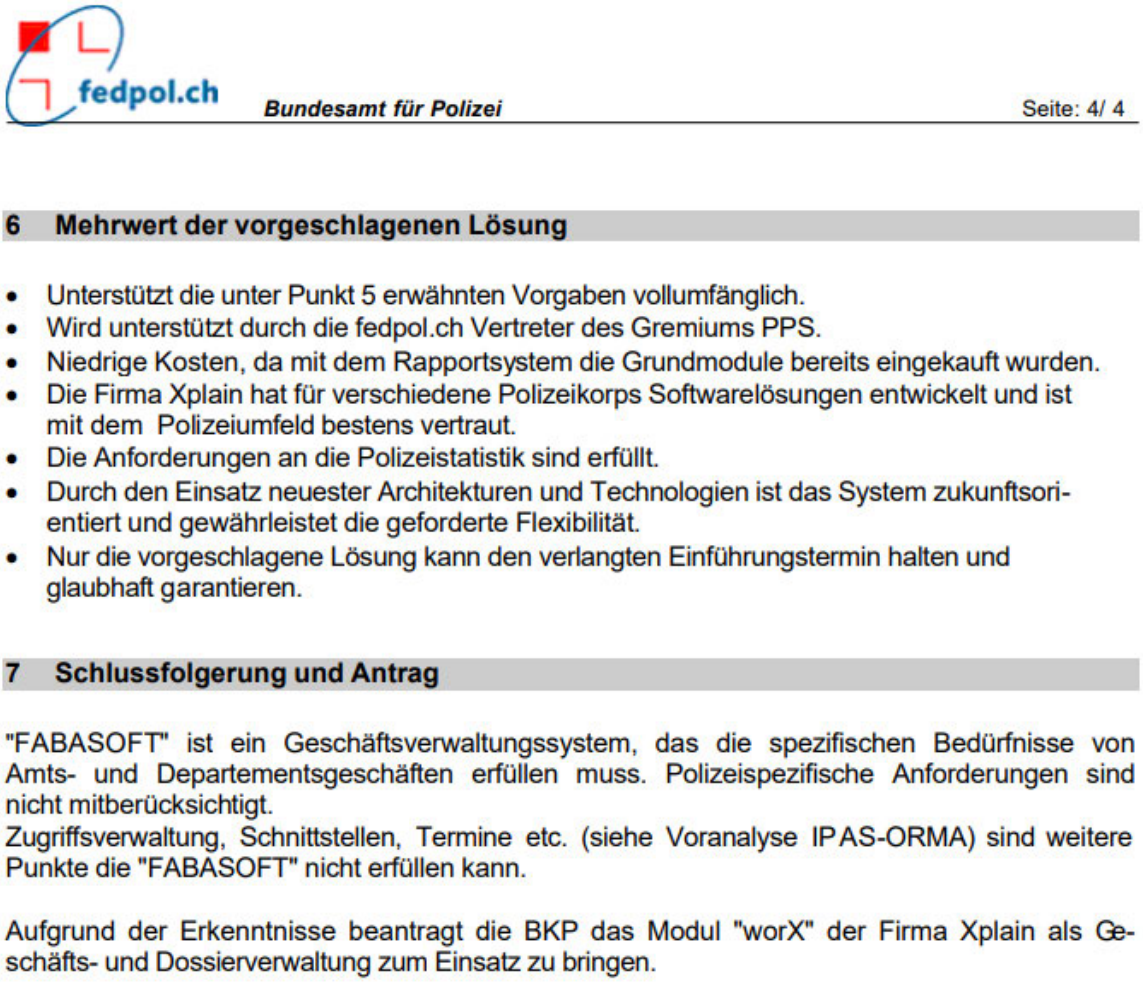
202 L'abréviation IPAS se réfère à un système d'information de fedpol: *Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem des Bundesamtes für Polizei*[129].

203 L'abréviation Janus se réfère à un système d'information de la PJF : *Elektronisches Informationssystem der Bundeskriminalpolizei*[130].

[127] FOSC, 04.07.2008 (128), n. 00311117.
[128] AUD 03.10.09.150-152.
[129] Fedpol, Rechenschatsbericht 2008, p. 47.
[130] Fedpol, Rechenschatsbericht 2008, p. 47.

204 L'abréviation PPS se réfère à l'unité « *Planung, Projektsteuerung und Standardisierung der Polizeilichen Informationsverarbeitung* » qui appartenait à la division des Ressources de fedpol jusqu'à fin 2008[131].

205 Le document contient enfin les points suivants[132] :



fedpol.ch **Bundesamt für Polizei** Seite: 4/ 4

6 Mehrwert der vorgeschlagenen Lösung

- Unterstützt die unter Punkt 5 erwähnten Vorgaben vollumfänglich.
- Wird unterstützt durch die fedpol.ch Vertreter des Gremiums PPS.
- Niedrige Kosten, da mit dem Rapportsystem die Grundmodule bereits eingekauft wurden.
- Die Firma Xplain hat für verschiedene Polizeikorps Softwarelösungen entwickelt und ist mit dem Polizeiumfeld bestens vertraut.
- Die Anforderungen an die Polizeistatistik sind erfüllt.
- Durch den Einsatz neuester Architekturen und Technologien ist das System zukunftsorientiert und gewährleistet die geforderte Flexibilität.
- Nur die vorgeschlagene Lösung kann den verlangten Einführungstermin halten und glaubhaft garantieren.

7 Schlussfolgerung und Antrag

"FABASOFT" ist ein Geschäftsverwaltungssystem, das die spezifischen Bedürfnisse von Amts- und Departementsgeschäften erfüllen muss. Polizeispezifische Anforderungen sind nicht mitberücksichtigt.
Zugriffsverwaltung, Schnittstellen, Termine etc. (siehe Voranalyse IPAS-ORMA) sind weitere Punkte die "FABASOFT" nicht erfüllen kann.

Aufgrund der Erkenntnisse beantragt die BKP das Modul "worX" der Firma Xplain als Geschäfts- und Dossierverwaltung zum Einsatz zu bringen.

206 Xplain a ensuite été choisie par fedpol pour développer l'application ORMA, utilisée au sein de fedpol dès février 2004[133] et qui a fait l'objet de plusieurs modifications et développements par Xplain depuis.

207 A partir de 2008, les relations entre la Confédération et Xplain se sont étendues à plusieurs unités et les contrats se sont multipliés. On citera principalement les projets :

- eneXs (OFDF, anc. AFD),
- ESYSP Los4 (CSI-DFJP/SEM/fedpol/DFAE),
- JORASYS (PM/BAC),
- ZEUSS (fedpol), et
- ZUPA/TROVA (OFJ).

[131] Fedpol, Rechenschatsbericht 2008, p. 7.
[132] 2003.04.29 Argumentarium Ausnahmegenehmigung.pdf (AUD 03.10.09.62)
[133] ORMA 2.3- Optimierungen – Pflichtenheft V1-0, p. 6 (AUD 03.10.09.158).

2. Collaboration

208 Les constatations suivantes peuvent être faites au sujet de la collaboration des Unités touchées par l'enquête avec Xplain.

209 De manière générale, l'Organe d'enquête ne dispose pas à ce jour d'une liste des contrats conclus entre les Unités touchées par l'enquête et Xplain qui revêtirait un caractère exhaustif. Au regard des réponses reçues des Unités touchées par l'enquête à nos demandes de renseignements et des réserves contenues dans certaines réponses, il n'est pas possible d'affirmer avec certitude que l'intégralité des contrats conclus entre la Unités touchées par l'enquête et Xplain ont été identifiés. Quoique la Confédération dispose d'un système de « *Vertragsmanagement* », nous comprenons que celui-ci ne contient pas nécessairement tous les contrats conclus avec un fournisseur externe donné. Ce constat appelle une recommandation qui sera exposée ci-dessous[134].

210 L'étendue des relations contractuelles entre la Confédération et Xplain peut être résumée comme suit sur la base des contrats remis à OA :

- fedpol était le service demandeur au sens de l'art. 3 let. b Org-OMP dans environ 100 contrats et avenants.
- L'OFJ était le service demandeur au sens de l'art. 3 let. b Org-OMP dans une trentaine de contrats et avenants.
- L'OFDF était le service demandeur au sens de l'art. 3 let. b Org-OMP dans une vingtaine de contrats et avenants.
- Le CSI-DFJP était le service demandeur au sens de l'art. 3 let. b Org-OMP dans cinq contrats.
- Le SEM était le service demandeur au sens de l'art. 3 let. b Org-OMP dans deux contrats. Le SEM a par ailleurs conclu avec le Cgfr un contrat en 2017 par lequel le Cgfr octroyait au SEM l'accès à certaines données du serveur eneXs du Cgfr.
- La BAC était le service demandeur au sens de l'art. 3 let. b Org-OMP dans trois contrats.
- armasuisse était le service d'achat central au sens de l'art. 3 let. a Org-OMP dans l'un des trois contrats précités dans lesquels la BAC était le service demandeur. armasuisse a également commandé des licences auprès de Xplain en lien avec Quattro P (cf. ci-dessous).
- L'OFCL était le service d'achat central au sens de l'art. 3 let. a Org-OMP dans certains contrats, mais pas tous, dans lesquels fedpol, l'OFJ, l'OFDF, le CSI-DFJP ou la BAC étai(en)t le(s) service(s) demandeur(s).
- Le DFAE n'a pas de relation contractuelle avec Xplain. Le DFAE a passé quatre commandes auprès de Xplain entre 2020 et 2022, qui se basaient sur le contrat-cadre précité entre Xplain et le CSI-DFJP (« Los 4 WTO 18021 »).
- L'OFIT n'a pas de relation contractuelle avec Xplain. A une occasion, en accord avec le SRC, l'OFIT a financé 16h de travaux de « *installation / deployment* » menés par Xplain en lien avec Quattro P (cf. ci-dessous)[135].
- La PM, qui est une unité organisationnelle du Commandement des Opérations (cdmt Op)[136], n'a pas de relation contractuelle avec Xplain. Elle est l'utilisatrice d'une application développée

[134] Cf. *infra* chapitre VI.B.
[135] AUD 03.06.28 ; AUD B03.06.36 ; AUD B03.06.37 ; AUD B03.06.38.
[136] Le cmdt Op est une unité administrative au sens de la OLOGA.

par Xplain (JORASYS) qui fait l'objet des contrats précités entre Xplain et la BAC (service demandeur).

- Le SRC n'a pas de relation contractuelle avec Xplain. Dans le cadre de Quattro P (art. 55 LRens), le SRC a accès à certaines données provenant de contrôles douaniers et de contrôles aux frontières.

211 La revue des contrats et les informations communiquées par les personnes interrogées nous conduisent par ailleurs à identifier, parmi les Unités touchées par l'enquête, celles qui utilisaient dans l'environnement informatique de la Confédération des produits développés par Xplain dans lesquels leurs données étaient traitées[137] :

- fedpol
- OFDF
- OFJ
- PM
- SEM

212 Ces unités sont désignées ci-après collectivement : les « Unités directement concernées ».

213 Tous les contrats remis à OA ont été conclus entre la Confédération et Xplain, soit la société anonyme dont le siège est à Interlaken[138]. De sources ouvertes et selon plusieurs interrogatoires, Xplain dispose de bureaux à Interlaken.

214 Selon son site internet, Xplain dispose en outre de bureaux à l'étranger, soit en Espagne et en Allemagne. A cet égard, de sources ouvertes également, il apparaît que deux des administrateurs de Xplain sont administrateurs, aux côtés d'autres personnes, d'une société Xplain AG Ibérica S.L., à Madrid[139].

215 Une offre présentée en 2020 par Xplain dans le cadre d'une demande d'offres de l'OFDF intitulée « Personenverwaltung ID-Center » indique que les deux sociétés suivantes sont « *im Besitz der Xplain AG und von Mitarbeitern* »[140] :

- Xplain AG Ibérica s.L, à Madrid (ES), fondée en 2011 et dirigée par Daniel Löwinger. Le document précise : « *In der Niederlassung Madrid werden Server- und Clientkomponenten sowie mobile Systeme entwickelt. Ein zweites Büro der Xplain AG Ibérica s.L. befindet sich in Ciudad Real. Dort werden wie in Madrid, Server- und Clientkomponenten entwickelt.* »
- deXplain GmbH, à Markkleeburg (DE), fondée en 2013 et dirigée par Sebastian Becker. Le document précise : « *In der Niederlassung Markkleeberg/Leipzig werden u.a. spezialisierte Biometrie-Lösungen entwickelt* ».

216 L'offre précitée de Xplain utilise le terme de « *Niederlassungen* » (succursales) pour décrire ces sociétés en Espagne et en Allemagne. Il s'agit toutefois de filiales (« *Tochtergesellschaften* ») puisque, au risque

[137] Le SRC recevait des données provenant d'un produit développé par Xplain, mais n'y entrait pas ses propres données (enregistrement audio de l'interrogatoire n° 231116-001, à partir de 6'20 et également à partir de 37'30).
[138] IDE : CHE-105.545.833.
[139] AUD 13.02.22-23.
[140] AUD 03.10.09.264-265.

d'énoncer une évidence, une « S.L. »[141] régie par le droit espagnol et une « GmbH » régie par le droit allemand, sont des personnes morales dotées de la personnalité juridique[142].

217 Toujours selon le même document, 21 personnes travaillaient à Interlaken, 33 à Madrid et une à Leipzig.

218 En résumé, les personnes interrogées à ce sujet ont indiqué, pour certaines, qu'elles ignoraient que Xplain avait des bureaux à l'étranger et, pour les autres, qu'elles connaissaient cette circonstance mais que, en substance, celle-ci relevait de choix organisationnels internes à Xplain et qu'il ne s'agissait pas d'un élément pertinent pour les relations entre Xplain et la Confédération.

219 Les cas de transmission de données productives à Xplain qui ont été analysés[143] sont intervenus dans le cadre de projets.

220 Ces projets étaient encadrés par une documentation contractuelle qui présente une forte hétérogénéité entre les unités et, au sein d'une unité, selon la date à laquelle ils ont été conclus, étant observé que plus de 150 contrats et avenants nous ont été remis et que les plus anciens remontent au début des années 2000.

221 Les contrats présentent cependant certains traits communs :

- Tous les contrats renvoient à des conditions générales de la Confédération et excluent les conditions générales d'Xplain.
- Aucun des contrats ne contient de clause aux termes de laquelle Xplain serait chargée d'effectuer un traitement de données[144]. Les prestations attendues d'Xplain sont, alternativement ou cumulativement, le conseil, la livraison, la maintenance, le support ou le développement de logiciels.

222 Nous reviendrons sur le contenu des contrats dans l'analyse juridique ci-dessous[145].

223 S'agissant de la correspondance entre les Unités directement concernées et Xplain, dans les cas de mise à disposition de données productives qui ont été analysés plus haut[146], nous n'avons identifié aucune instruction donnée à Xplain en lien avec la mise à disposition ou l'effacement des données en question.

224 Par ailleurs, nous n'avons identifié aucun audit ou rapport sur la sécurité de l'information ou la protection des données au sein d'Xplain.

225 A la connaissance des personnes interrogées sur cette question, Xplain n'a jamais fait l'objet d'un audit de la Confédération en matière de sécurité de l'information ou de protection des données.

V. APPRÉCIATION JURIDIQUE DES FAITS

226 La présente enquête administrative porte sur des faits qui se sont déroulés sur une période de près de 25 ans. Durant cette période, les règles de droit pertinentes ont connu de nombreux changements.

---

[141] « *Sociedad de responsabilidad limitada* ».

[142] Art. 1 et 33 Ley de Sociedades de Capital (Real Decreto Legislativo 1/2010, de 2 de julio ; dernière modification 29.06.2023 ; référence BOE-A-2010-10544) ; § 13 GmbH-Gesetz (Gesetz betreffend die Gesellschaften mit beschränkter Haftung ; dernière modification 22.02.2023 ; BGBl. I S. 3436).

[143] Cf. *supra* chapitre IV.A.

[144] Xplain a adressé en novembre 2022 une offre à la Police militaire concernant l'archivage des évènements JORASYS du 01.01.1900 au 31.01.2013, qui n'a apparemment pas été acceptée par la Police militaire (e-mail du 1er décembre 2022, AUD 03.10.09.167-172).

[145] Cf. *infra* chapitre V.A.

[146] Cf. *supra* chapitre IV.A.

227 Les faits sous enquête sont analysés à la lumière des règles applicables lorsqu'ils se sont produits. Cela étant, dans la perspective de tirer des enseignements et de formuler des propositions (*infra* chapitre VI), il nous paraît nécessaire de présenter également les règles de droit en vigueur à la date du présent rapport, soit le 28 mars 2024.

228 Le présent rapport n'a pas pour objet ou pour ambition de traiter exhaustivement les règles de droit passées et présentes relatives à la sécurité de l'information ou la protection des données. L'examen se concentre sur les questions posées dans le mandat d'enquête, qui peuvent être résumées comme suit (sections A et B ci-dessous).

A. Est-ce que des déficiences en matière technique, d'organisation ou de processus au sein de la Confédération ont conduit à ce que Xplain AG se trouve en possession de données productives de la Confédération ?

229 Après avoir exposé les règles de droit pertinentes (*infra* ch. 1), nous procéderons à l'analyse juridique des faits qui ont pu être établis (*infra* ch. 2).

230 Concrètement, nous examinerons certains exemples de transmission de données productives vers Xplain par les canaux qui ont été identifiés au chapitre IV.A. Dans les cas où la présence de données productives dans l'environnement informatique de Xplain est établie, mais où le canal expliquant la présence de ces données n'a pas pu être identifié, l'analyse juridique reposera sur des hypothèses.

231 Lors de l'analyse de chaque cas, nous examinerons, dans un premier temps, la compatibilité de la transmission des données en question avec le droit en vigueur à l'époque (à l'exclusion du droit pénal) et, dans un second temps, l'existence de déficiences en matière technique, d'organisation ou de processus.

1. Règles de droit pertinentes

a) Remarques introductives

232 La question posée nécessite quelques explications générales sur le cadre légal dans lequel elle s'inscrit (*infra* b). Nous listerons ensuite les principales lois et ordonnances législatives abrogées dans les matières qui nous intéressent (*infra* c). Nous passerons enfin en revue les principaux thèmes traités par les règles de droit pertinentes (*infra* d).

233 A titre liminaire, il convient également d'expliquer la démarche consistant ne pas exposer les ordonnances administratives (notamment : directives, circulaires ou instructions) dans le présent survol des règles de droit, mais dans la partie consacrée à l'analyse du cas d'espèce (*infra* ch. 2).

234 Les ordonnances administratives[147], qui se distinguent notamment des ordonnances législatives[148], s'adressent aux agents de l'administration et leur prescrivent la façon dont ils doivent accomplir leurs tâches. Les ordonnances administratives poursuivent les objectifs les plus divers de nature administrative

[147] La fonction principale de ces ordonnances est de garantir l'unification et la rationalisation de la pratique. Ce faisant, elles permettent également d'assurer l'égalité de traitement et la prévisibilité administrative et facilitent aussi le contrôle juridictionnel (ATF 131 V 42 consid. 2.3; ATAF 2009/15 consid. 5.1).

[148] Par ordonnances législatives, on entend celles qui s'adressent, tout comme les lois, à l'ensemble des autorités et des particuliers et contiennent des règles de droit. Pour être opposables aux particuliers, les ordonnances législatives doivent être publiées (parmi d'autres, cf. arrêt du TAF A-5446/2016 du 23 mai 2018 consid. 3.1.4).

et organisationnelle[149]. Elles n'ont pas force de loi et ne lient ni les administrés, ni les tribunaux, ni même, à proprement parler l'administration[150], quoique leur caractère impératif connaisse des degrés d'intensité variables[151] (notamment : l'autorité administrative subordonnée est en principe liée par le texte édicté par l'autorité hiérarchique, ce texte pouvant au surplus affecter, parfois même directement, la situation juridique des administrés) ; elles ne sont impératives pour les autorités d'application de la loi que dans la mesure où elles restituent le sens exact de celle-ci[152]. Elles ne dispensent pas l'administration de se prononcer à la lumière des circonstances du cas d'espèce et ne peuvent pas sortir du cadre fixé par la norme supérieure qu'elles sont censées concrétiser. A défaut de lacune, les ordonnances administratives ne peuvent prévoir autre chose que ce qui découle de la législation ou de la jurisprudence[153].

235 Les ordonnances administratives n'ont donc pas force de loi ; pour des motifs de systématique, il n'y a donc pas lieu de les présenter dans les règles de droit. Les ordonnances administratives seront ainsi discutées lors de l'analyse des cas concrets, au moment d'examiner d'éventuelles déficiences en matière technique, d'organisation ou de processus.

b) Cadre légal

236 Examiner si des déficiences en matière technique, d'organisation ou de processus au sein de la Confédération ont conduit à ce que Xplain AG se trouve en possession de données productives de la Confédération, soulève de manière générale la question de la sécurité de l'information (*i*). Selon le type de données concernées, cela soulève en particulier la question de la classification des informations (*ii*). En outre, ici encore selon le type de données concernées, la législation sur la protection des données peut trouver application (*iii*).

237 En revanche, l'analyse des faits sous l'angle du droit pénal ne fait pas partie du mandat, conformément à la nature de l'enquête administrative (art. 27*a* OLOGA) et à la demande d'offres du 21 juillet 2023, auquel renvoie le contrat entre la Confédération et OA.

(i) *Sécurité de l'information*

238 La sécurité de l'information englobe toutes les exigences et mesures visant à protéger la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations et données de tout type, de même que la disponibilité et l'intégrité des moyens informatiques[154].

239 La loi sur la sécurité de l'information (LSI), entrée en vigueur le 1er janvier 2024 et qui s'applique en particulier à l'administration fédérale et à l'armée (art. 2 al. 2 let. b et d LSI), poursuit deux objectifs :

1. Elle regroupe en un seul acte les bases légales principales régissant la sécurité des informations et des moyens informatiques de la Confédération, lesquelles étaient jusqu'alors disséminées,

[149] En allemand, on retrouve par exemple les termes suivants : « *Direktiven, Weisungen, Dienstanweisungen, Dienstreglemente, allgemeine Dienstbefehle, Rundschreiben, Kreisschreiben, Zirkulare, Wegweisungen, Anleitungen, Instruktionen, Merkblätter, Leitbilde* » ; cf. ATF 128 I 167 consid. 4.3. Le plus souvent, les ordonnances administratives sont adoptées par les Départements, voire par les offices fédéraux et ne sont en principe pas publiées.
[150] ATF 141 V 175 consid. 2.1 ; ATF 133 II 305 consid. 8.1 ; THIERRY TANQUEREL, Manuel de droit administratif, 2e éd., 2018, N 331 p. 115.
[151] PIERRE MOOR/ALEXANDRE FLÜCKIGER/VINCENT MARTENET, Droit administratif, vol. I : Les fondements, 3e éd., 2012, p 398.
[152] ATF 142 II 182 2.3.2.
[153] ATF 141 V 175 consid. 4.1, 138 II 536 consid. 5.4.3; arrêts du TAF A-1412/2015, A-1422/2015 du 14 décembre 2016 consid. 4, A-4357/2015 du 10 juillet 2017 consid. 2.5.
[154] Secrétariat général du DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information – Explications, 8 novembre 2023, p. 2.

généralement sans précision, dans une multitude d'actes (p. ex. LOGA, LParl, LAAM, CP, LMSI, LPers, LMP, LAr, LPD, LTrans) qui ne s'appliquaient qu'à certaines autorités[155].

2. Elle s'applique à l'ensemble des autorités et organisations de la Confédération, afin d'atteindre un niveau de sécurité aussi homogène que possible[156].

240 De manière générale, la LSI (art. 6 al. 1) prévoit pour principe que les autorités et organisations soumises à la LSI veillent à ce que le besoin de protection des informations relevant de leur compétence soit évalué en fonction de l'atteinte potentielle aux intérêts publics définis. Le besoin spécifique de protection à raison de la matière est très souvent implicitement déterminé par d'autres lois[157]. Sur le plan matériel, l'art. 6 al. 2 LSI, qui se calque sur la doctrine et la pratique, retient quatre critères de protection pour la sécurité de l'information (confidentialité ; disponibilité ; intégrité et traçabilité). Par exemple, le maintien de la confidentialité n'est nécessaire que si elle doit être garantie pour une raison légale. Certaines informations peuvent justifier des exigences accrues en matière de protection de leur intégrité ou de leur disponibilité, sans pour autant que de telles exigences figurent explicitement dans la législation, notamment lorsque ces informations doivent impérativement être exactes ou disponibles pour l'accomplissement des tâches d'une autorité. Cela concerne en particulier les informations et les moyens informatiques qui soutiennent des processus critiques des autorités[158].

241 Les autorités et organisations concernées veillent à ce que les moyens informatiques auxquels elles recourent pour accomplir leurs tâches légales soient protégés contre les utilisations abusives et les perturbations (art. 6 al. 3 LSI).

242 L'art. 17 LSI prévoit les catégories de sécurité (« protection de base » ; « protection élevée » ; « protection très élevée ») visent à identifier, sous l'angle des intérêts publics au sens de l'art. 1 al. 2 LSI, la criticité d'un moyen informatique déterminé. La criticité découle de la gravité du préjudice que peuvent causer les informations traitées avec le moyen informatique concerné ou le moyen informatique lui-même lorsqu'ils sont utilisés abusivement ou perturbés. Dès lors, la catégorisation dépend tant des besoins de protection de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des informations que de la criticité du déroulement adéquat et sans retard des processus d'affaires soutenus par le moyen informatique[159].

243 Selon le Message, la LSI ne fixe toutefois aucune mesure précise pour garantir la sécurité de l'information, mais pose uniquement un cadre formel sur la base duquel les autorités fédérales prendront les mesures de sécurité de l'information par voie d'ordonnance et de directive[160]. Conformément à l'art. 85 LSI, le Conseil fédéral est chargé de fixer des exigences et des mesures standard en fonction des connaissances scientifiques et techniques les plus récentes. La disposition ne vise pas des exigences et des mesures organisationnelles de base, qui seront définies au niveau de l'ordonnance, mais principalement des exigences de nature secondaire ou technique[161]. De nombreux États ou organisations internationales ont

[155] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2776.
[156] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765 2766 s.
[157] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2827.
[158] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2828.
[159] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2836.
[160] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765 2766 s.
[161] Le message fournit des exemples (norme pour l'évaluation du besoin de protection des informations sous l'angle des quatre critères mentionnés à l'art. 6 al. 2 ; méthode standard pour l'évaluation des risques; normes pour les mesures à prendre aux niveaux de l'organisation, du personnel, de la technique et des constructions (art. 8); normes pour des processus et des moyens particuliers destinés à protéger des informations classifiées (art. 11 à 15); normes pour la protection de base, l'élaboration de

déjà défini des normes dans leur domaine. « *Les autorités fédérales ne seront dès lors pas obligées de réinventer la roue* »[162]. Selon le Message, le Conseil fédéral pourra, si nécessaire, pour ne pas devoir ordonner des mesures opérationnelles techniques, déléguer l'élaboration et l'adoption des normes à des services subordonnés, à la Conférence des secrétaires généraux (art. 53 LOGA), au service spécialisé de la Confédération pour la sécurité de l'information, ou encore à fedpol dans le domaine de la protection des objets[163].

244 Selon l'art. 4 al. 2 LSI, « *[l]orsque la protection d'informations est également réglée dans d'autres lois fédérales, les dispositions de la présente loi s'appliquent à titre complémentaire*. »

245 Parmi ces « autres lois fédérales » figure la LPD entrée en vigueur le 1er septembre 2023. Alors que la LSI vise tous les types d'informations et de données, le champ d'application matériel de la LPD est limité aux données personnelles, soit « *toutes les informations concernant une personne physique identifiée ou identifiable* » (art. 5 let. a LPD).

246 La LPD prévoit que les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru (art. 8 al. 1 LPD). Les mesures doivent permettre d'éviter toute violation de la sécurité des données (al. 2). Cette disposition matérialise l'approche fondée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées[164].

247 En complément, l'art. 2 OPDo impose au responsable du traitement et au sous-traitant de prendre des mesures pour la protection de la confidentialité, de la disponibilité, de l'intégrité des données et de la traçabilité par la sécurité des données (art. 2 OPDo)[165]. L'art. 3 OPDO définit ces mesures techniques et organisationnelles.

(ii) *Classification des informations*

248 La classification des informations est l'une des mesures de la LSI destinées à protéger les informations[166].

249 Toutes les informations ne sont pas classifiées. La classification est obligatoire dès lors que les critères afférents sont remplis (cf. art. 11 LSI). L'art. 13 LSI règle les conditions matérielles de la classification des informations et fixe les échelons de classification correspondants pour toutes les autorités et organisations soumises à la LSI.

250 Les échelons de classification sont les suivants :

- interne
- confidentiel
- secret

251 Ils sont déterminés par la gravité du préjudice que la divulgation des informations à une personne non autorisée peut porter aux intérêts définis à l'art. 1 al. 2 let. a à d LSI (divulgation susceptible de *nuire à*

plan de sécurité de l'information et la sécurité des moyens informatiques des catégories «protection élevée» et « protection très élevée » (art. 16 à 19) (Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2879).

[162] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2879.

[163] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2879.

[164] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6650.

[165] NICOLAS BEGUIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 1 ad art. 8 LPD.

[166] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2790.

ces intérêts [« interne »] ; divulgation susceptible de *nuire considérablement à ces intérêts* [« confidentiel »] ; divulgation susceptible de *nuire gravement à ces intérêts* [« secret »]).

252 Avec la LSI, les informations classifiées « confidentiel » selon l'ancienne OPrI tendent désormais à entrer dans la catégorie « interne ». Selon le Conseil fédéral, cela devrait réduire massivement le nombre d'informations classifiées et, entre autres, diminuer le nombre de contrôles de sécurité relatifs aux personnes (PSP)[167].

(iii) *Protection des données*

253 Alors que la LSI protège des intérêts publics et certains intérêts de la Confédération en sa qualité d'institution (art. 1 al. 2 LSI)[168], la LPD vise à protéger la personnalité (art. 28 CC) et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement (droit à la liberté personnelle [art. 10 al. 2 Cst] ; droit à la vie privée [art. 13 al. 1 Cst.] ; droit à l'autodétermination informationnelle [art. 13 al. 2 Cst. et art. 8 CEDH])[169].

254 La protection des données personnelles par des organes fédéraux est régie pour l'essentiel par la LPD et l'OPDo, respectivement par les art. 57*h* ss LOGA. Par ailleurs, depuis l'entrée en vigueur de la LPD le 1er septembre 2023, le traitement des données des personnes morales par des organes fédéraux relève des art. 57*r* ss LOGA[170].

255 La LPD prévoit en particulier que des données personnelles ne peuvent être collectées que de façon licite et dans le respect du principe de la proportionnalité et pour des finalités déterminées et reconnaissables, et être traitées ultérieurement de manière compatible avec ces finalités (art. 6 al. 1-3 LPD).

c) Historique des actes essentiels abrogés

256 Le tableau ci-dessous liste les principales lois et ordonnances législatives abrogées. Ce tableau illustre l'éclatement des règles juridiques auxquelles la LSI a toutefois apporté une systématique dès le 1er janvier 2024.

[167] Chancellerie fédérale, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, 31 août 2022, p. 32.
[168] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2822.
[169] JULIEN FRANCEY, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 11 ad art. 1 LPD.
[170] La LPD introduit dans la LOGA un certain nombre de dispositions légales concernant le traitement de données concernant des personnes morales par des organes fédéraux. En effet, en raison de l'abrogation de la protection des données des personnes morales dans la LPD, les bases légales prévues par le droit fédéral qui habilitaient les organes fédéraux à traiter des données personnelles ne s'appliquent plus lorsque ceux-ci traitent des données concernant des personnes morales depuis le 1er janvier 2024. Les art. 5, 13, al. 2, et 36 Cst. sont ainsi respectés (Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6063, 6733).

<table>
<tr><th>Sécurité des informations (y compris classification)</th><th>Informatique / Télécommunication</th><th>Cyberrisques</th><th>Protection des données</th></tr>
<tr>
<td>Ordonnance du 1er mai 1990 concernant la protection des informations militaires (Ordonnance concernant la protection des informations) (anciennement au RS 510.411)
<table><tr><td>Entrée en vigueur</td><td>1er janvier 1991[171]</td></tr><tr><td>Date d'abrogation</td><td>1er août 2007[172]</td></tr><tr><td>Remplacée par</td><td>Ordonnance concernant la protection des informations, aOPrI</td></tr></table></td>
<td>Ordonnance du 23 février 2000 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, aOIAF)
<table><tr><td>Entrée en vigueur</td><td>1er avril 2000[173]</td></tr><tr><td>Date d'abrogation</td><td>1er octobre 2003[174]</td></tr><tr><td>Remplacée par</td><td>Ordonnance du 26 septembre 2003 sur l'informatique dans l'administration fédérale</td></tr></table></td>
<td>Ordonnance du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, aOPCy)
<table><tr><td>Entrée en vigueur</td><td>1er juillet 2020[175]</td></tr><tr><td>Date d'abrogation</td><td>1er janvier 2024[176]</td></tr><tr><td>Remplacée par</td><td>Ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)</td></tr></table></td>
<td>Loi fédérale du 19 juin 1992 sur la protection des données (aLPD)
<table><tr><td>Entrée en vigueur</td><td>1er juillet 1993[177]</td></tr><tr><td>Date d'abrogation</td><td>1er septembre 2023[178]</td></tr><tr><td>Remplacée par</td><td>Loi fédérale du 25 septembre 2020 sur la protection des données (LPD)</td></tr></table></td>
</tr>
<tr>
<td>Ordonnance du 10 décembre 1990 sur la classification et le traitement d'informations de l'administration civile (anciennement au RS 172.015)
<table><tr><td>Entrée en vigueur</td><td>1er janvier 1991[179]</td></tr><tr><td>Date d'abrogation</td><td>1er août 2007[180]</td></tr><tr><td>Remplacée par</td><td>Ordonnance du 4 juillet 2007 concernant la protection des informations (aOPrI)</td></tr></table></td>
<td>Directives du Conseil fédéral du 23 février 2000 concernant l'informatique et la télécommunication dans l'administration fédérale (Directives informatiques du Conseil fédéral, aDITAF)
<table><tr><td>Entrée en vigueur</td><td>1er avril 2000[181]</td></tr><tr><td>Date d'abrogation</td><td>1er octobre 2003[182]</td></tr><tr><td>Remplacées par</td><td>Ordonnance du 26 septembre 2003 sur l'informatique dans l'administration fédérale</td></tr></table></td>
<td></td>
<td></td>
</tr>
</table>

[171] RO 1990 887.
[172] RO 2007 3401.
[173] RO 2000 1227.
[174] RO 2003 3687.
[175] RO 2020 2107.
[176] RO 2023 735.
[177] RO 1993 1945.
[178] RO 2022 491.
[179] RO 1991 44.
[180] RO 2007 3401.
[181] RO 2000 2708.
[182] RO 2003 3687.

Ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération (Ordonnance concernant la protection des informations, aOPrI) (anciennement au RS 510.411] Entrée en vigueur: 1er août 2007[183] Date d'abrogation: 1er janvier 2024 Remplacée par: OSI[184]	Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, aOIAF) Entrée en vigueur: 1er octobre 2003[185] Date d'abrogation: 1er janvier 2012[186] Remplacée par: Ordonnance du 9 décembre 2011 sur l'informatique dans l'administration fédérale (aOIAF).		
	Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, aOIAF) (anciennement au RS 172.010.58) Entrée en vigueur: 1er janvier 2012[187] Date d'abrogation: 1er janvier 2021[188] Remplacée par: Ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI)[189]		

[183] RO 2007 3401.
[184] Ordonnance du 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (Ordonnance sur la sécurité de l'information, OSI) (RS 128.1) (entrée en vigueur le 1er janvier 2024 [RO 2023 735]). Selon un rapport explicatif, l'OSI remplace l'ordonnance du 27 mai 2020 sur les cyberrisques (aOPCy) et l'ordonnance du 4 juillet 2007 concernant la protection des informations (aOPrI) (cf. SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif, 24 août 2022, p. 6).
[185] RO 2003 3687.
[186] RO 2011 6093.
[187] RO 2011 6093.
[188] RO 2020 5871.
[189] Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (Ordonnance sur la transformation numérique et l'informatique, OTNI) (RS 172.010.58) (entrée en vigueur le 1er janvier 2021 [RO 2020 5871]).

d) Principales règles

257 Les lois et ordonnances législatives actuellement en vigueur posent les règles principales suivantes, qui sont potentiellement pertinentes au vu de la question posée.

(i) *Principe de la légalité*

258 Dans la matière qui nous intéresse, le principe de la légalité est ancré à l'art. 34 al. 1 LPD[190] (art. 17 al. 1 aLPD), en vertu duquel les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale.

259 L'exigence de la base légale en cas de traitement de données personnelles par des organes fédéraux (art. 5 let. i LPD) vise à la fois à donner une légitimité démocratique à l'action de l'Etat, à poser des limites aux mesures étatiques (cadre légal), tout en assurant prévisibilité du droit et égalité de traitement ; dans ce sens, l'exigence garantit une certaine transparence[191].

260 Le degré de précision (densité normative) de la base légale doit être proportionné à la gravité de l'atteinte au droit fondamental. La base légale doit permettre à la personne concernée de connaître

- quel organe fédéral traite
- quelle catégorie de données,
- dans quel but,
- qui a accès aux données,
- à qui les données peuvent être communiquées et
- dans quel but,
- ainsi que l'étendue du traitement dans les grandes lignes[192].

261 La base légale doit être prévue dans une loi au sens formel en particulier s'il s'agit d'un traitement de données personnelles sensibles (art. 5 let. c LPD) ou si la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 34 al. 2 let. a et c LPD).

262 L'art. 57*h*^{bis} al 1 LOGA autorise le traitement de données personnelles dans la perspective du bon déroulement des processus opérationnels (système de gestion des affaires). La base légale pour le traitement (particulièrement la collecte et la communication) de données personnelles doit néanmoins toujours découler du droit spécial applicable aux données en question[193].

263 Toutefois, lorsqu'un organe fédéral agit selon le droit privé, le traitement des données personnelles est régi par les dispositions applicables aux personnes privées (art. 40 LPD), soit en particulier les art. 5 à 32 LPD[194]. Or, les personnes privées agissent librement tant que la loi ne leur fixe pas de limites, le régime étant ainsi, sous cet angle, moins strict pour les personnes privées que pour les organes fédéraux[195].

---

[190] La norme concrétise le principe de la légalité au sens des art. 5 et 164 Cst. et prend en compte l'art. 36 al. 1 Cst., qui prévoit que toute restriction d'un droit fondamental doit être fondée sur une base légale (cf. MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 2 ad art. 34 LPD).

[191] MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 10 ad art. 34 LPD.

[192] OFJ, Guide de législation Guide pour l'élaboration de la législation fédérale, 4e éd., 2019, p. 213, N 824 ; MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 12 ad art. 34 LPD.

[193] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6063, 6731.

[194] Cf. ci-dessous par. 285.

[195] MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 9 ad art. 34 LPD.

264 La distinction entre activité privée et activité relevant de la puissance publique (soit, d'un organe fédéral) au sens de la LPD n'est pas toujours évidente. Relèvent notamment d'une activité de droit privé les activités commerciales déployées par les établissements autonomes de droit public, les activités de support administratif telles que l'acquisition de bien (par exemple le matériel de bureau) ou de services (par exemple l'entretien des bureaux) ou encore l'exercice d'une activité commerciale[196].

(ii) *Principe de proportionnalité*

265 Tout traitement de données (personnelles ou non) doit respecter le principe de proportionnalité (art. 5 al. 2 Cst. et 36 al. 3 Cst. ; cf. également art. 6 al. 2 LPD et 6 al. 4 LSI)[197].

266 En matière de protection des données personnelles, les principes d'évitement et de minimisation des données constituent deux expressions du principe de la proportionnalité. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée. Le second veut que seules les données absolument nécessaires au but poursuivi soient traitées[198] (cf. également principe de finalité [art. 6 al. 3 LPD]).

(iii) *Débiteur de l'obligation de protection des informations et responsabilité des autorités*

267 En matière de protection des données personnelles, le responsable du traitement (organes fédéraux), le cas échéant le sous-traitant[199], est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'art. 6. Il le fait dès la conception du traitement (art. 7 al. 1 LPD ; « *privacy by design* »).

268 Dans le champ d'application de la LSI, les autorités veillent, chacune dans son domaine de compétence, à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques (art. 7 al. 1 LSI).

269 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités administratives visées à l'art. 2, al. 1, let. c OSI, sont responsables de la sécurité de l'information dans leur domaine de compétence (art. 36 al. 1 OSI). Toutefois, ils peuvent déléguer la responsabilité en matière de sécurité de l'information à un membre de la direction s'il dispose des pouvoirs nécessaires pour prendre des mesures, les contrôler et les corriger (art. 36 al. 2 OSI).

270 Ainsi, la sécurité est de la responsabilité de la hiérarchie. Les autorités soumises à la LSI doivent organiser, mettre en œuvre et contrôler la sécurité de l'information dans leur domaine de compétence, en tenant compte des connaissances scientifiques et techniques les plus récentes. Plusieurs normes formulent ce qui est communément appelé bonnes pratiques dans la gestion de la sécurité de l'information et fixent des exigences pour l'application de mesures de sécurité adaptables aux besoins des diverses autorités ou organisations[200].

271 Par exemple, la loi ne commande pas aux autorités de mettre en place un système de gestion de la sécurité de l'information selon la norme DIN ISO/IEC 27001, mais leur organisation devrait au moins s'en inspirer[201].

---

[196] TEO GÉNÉCAND, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 4 s. ad art. 40 LPD.
[197] ATF 138 II 346 consid. 9.2.
[198] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6644.
[199] NICOLAS BEGUIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 11 ad art. 7 LPD.
[200] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2828 s.
[201] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2828 s.

(iv) *Sécurité des données personnelles : mesures organisationnelles et techniques*

272 La protection des données personnelles relève de la protection de la personnalité de l'individu. Quant à la sécurité des données personnelles, elle vise généralement les données présentes chez un responsable du traitement ou chez un sous-traitant et englobe le cadre organisationnel et technique général du traitement des données[202].

273 Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques (« MOT » ; connues également sous l'acronyme TOMs [« *technical and organisational measures* ») appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru (art. 8 al. 1 LPD ; art. 7 al. 1 aLPD). Les mesures doivent permettre d'éviter toute violation de la sécurité des données (art. 8 al. 2 LPD) (cf. art. 3 OPDo).

274 L'art. 8 LPD oblige tant le responsable du traitement que le sous-traitant à prévoir, pour leurs systèmes, une architecture de sécurité appropriée et à les protéger contre les maliciels ou la perte de données, par exemple[203].

275 A titre d'exemples de mesure techniques, l'on peut citer le cryptage, le chiffrement, la pseudonymisation de données, la protection par mot de passe, la mise en place d'un système de sauvegarde régulier, l'enregistrement de l'identité de personnes consultant certains types de données ou le recours à un protocole chiffré HTTPS[204].

276 Les mesures organisationnelles concernent la structure et les procédures mises en place au sein d'un organe fédéral pour satisfaire au principe de sécurité des données (p. ex. formation du personnel et des sous-traitants éventuels, élaboration de règles de conduite des employés ou d'évaluation de l'efficacité des mesures prises, délimitation des tâches, des fonctions et des responsabilités en matière de sécurité des données ou établissement d'un plan de réponse en cas de faille de sécurité)[205].

277 Le PFPDT a publié à ce propos un Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM) du 15 janvier 2024. Le guide détaille principalement les obligations des responsables de traitement privés, mais les responsables de traitement d'un organe fédéral pourront également trouver des informations spécifiques les concernant dans la section « Organes fédéraux » dudit guide.

(v) *Gestion des risques*

278 En matière de sécurité des données personnelles, l'art. 8 LPD (art. 7 aLPD) concrétise l'approche fondée sur les risques. Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées (sécurité adéquate des données personnelles par rapport au risque encouru)[206].

279 Selon la LSI, les autorités et organisations concernées veillent, chacune dans son domaine de compétence, à ce que les risques en matière de sécurité de l'information soient constamment évalués

[202] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6650.
[203] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6650.
[204] NICOLAS BEGUIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 10 ad art. 8 LPD.
[205] NICOLAS BEGUIN, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 11 ad art. 8 LPD.
[206] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2789.

(art. 8 al. 1 LSI). Elles prennent les mesures nécessaires pour éliminer les risques ou les ramener à un niveau acceptable (art. 8 al. 2 LSI). Les risques jugés acceptables doivent être formellement acceptés (art. 8 al. 3 LSI).

280 L'évaluation des risques présuppose une solide connaissance des tâches légales et des processus d'affaires qui s'y rapportent, une appréciation régulière des menaces, l'analyse des vulnérabilités, la détermination de la probabilité de survenance d'un événement et l'estimation des dommages potentiels liés à des risques donnés[207]. Un objectif important de la gestion des risques est de prendre les mesures les plus efficaces pour éviter ou réduire les risques. Les risques peuvent être évités dans la mesure où l'on peut renoncer totalement à une activité trop risquée (p. ex. renoncer à un projet informatique pour lequel l'application de mesures de prévention des risques n'est pas défendable économiquement)[208].

281 Les risques peuvent également être pris en compte ou supportés, mais ils ne devraient pas être ignorés. Les risques subsistant après l'application des mesures de sécurité prévues (appelés risques résiduels) et les risques ne devant pas être minimisés doivent être clairement signalés. Les décideurs doivent être pleinement avisés de ces risques et de leurs conséquences potentielles. Les risques résiduels doivent être clairement acceptés et supportés[209].

282 Selon le Message, des mesures organisationnelles, plus efficaces ou plus économiques, sont régulièrement développées dans le domaine de la sécurité de l'information. Les évolutions techniques sont encore plus rapides, notamment en ce qui concerne les moyens informatiques. Il est très important que les mesures de sécurité ne reposent pas sur des technologies obsolètes et qu'elles agissent contre les menaces d'aujourd'hui. Les normes doivent donc être élaborées selon les connaissances scientifiques et techniques les plus récentes (cf. art. 85 LSI), tout en sachant que les critères d'acceptation des risques déterminants pour l'évaluation des risques sont fixés par chaque autorité soumise à la loi en fonction de ses propres besoins en matière de sécurité de l'information[210].

(vi) *Communication (accès)*

283 *En matière de données personnelles*. Pour ce qui est de leur communication, la LPD prévoit que les organes fédéraux ne sont en droit de communiquer des données personnelles que si une base légale au sens de l'art. 34 al. 1 à 3 LPD le prévoit (art. 36 al. 1 LPD ; cf. aussi art. 57*h*^{bis} al 2 LOGA, qui prévoit la nécessité de disposer d'une base légale pour pouvoir communiquer des données personnelles ainsi que des données concernant des personnes morales[211]).

284 En dérogation à cette règle, ils peuvent, dans un cas d'espèce, communiquer des données personnelles si l'une des conditions prévues à l'art. 36 al. 2 LPD est remplie, parmi lesquelles l'on citera les cas suivants : a) la communication des données est indispensable à l'accomplissement des tâches légales du responsable du traitement ou du destinataire ; c) la communication des données est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable. Toutefois, les organes fédéraux refusent la communication, la restreignent ou l'assortissent de charges a) si un intérêt public

[207] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2830.
[208] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2830.
[209] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2830.
[210] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2830.
[211] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6731.

important ou un intérêt digne de protection manifeste de la personne concernée l'exige, ou b) si une obligation légale de garder le secret ou une disposition particulière de protection des données l'exige.

285 Si toutefois les organes fédéraux agissent selon le droit privé, le traitement des données personnelles est régi par les dispositions applicables aux personnes privées (art. 40 LPD). Dans cette hypothèse, une base légale ne sera pas nécessaire avant de communiquer des données personnelles et les organes fédéraux pourront, le cas échéant, se prévaloir des motifs justificatifs de l'art. 31 LPD[212].

286 Pour ce qui est de l'utilisation de l'infrastructure électronique de la Confédération, selon l'OTUIC, seuls ont droit d'accéder aux données administrées : a) l'exploitant du système ; b) les services désignés par les directives de l'organe fédéral concernant la protection des données (art. 2 al. 1). Seul l'organe fédéral qui utilise les appareils sur lesquels les données non administrées sont enregistrées a droit d'accéder à ces données (art. 2 al. 2).

287 *En matière d'information classifiées.* Pour ce qui est de l'accès aux informations classifiées, la LSI prévoit que seules peuvent accéder aux informations classifiées les personnes qui offrent toutes les garanties qu'elles les traiteront correctement et qui remplissent l'une des conditions suivantes: a) elles ont besoin des informations en question pour accomplir une tâche légale; b) elles disposent d'une autorisation d'accès qui leur a été conférée contractuellement et ont besoin des informations en question pour accomplir les tâches qui leur ont été confiées (art. 14 LSI).

288 Le principe du *besoin de connaître* les informations (« *need to know* ») vaut pour chaque information classifiée. Il n'existe donc pas de droit général à accéder à toutes les informations classifiées[213].

289 Ce principe s'applique également aux organes de vérification, de contrôle et de surveillance : bien qu'ils disposent d'un droit général à l'information dans les cas d'espèce, ils doivent justifier pour chaque information classifiée que les informations visées sont effectivement nécessaires à l'accomplissement de leurs tâches. Si le droit d'accès est convenu contractuellement, les accords conclus à cet effet doivent prévoir l'accès aux informations classifiées et régler leur traitement[214].

(vii) *Encadrement de la collaboration avec les tiers*

290 La sécurité de l'information régit les mesures qui doivent être prises pour que des personnes non autorisées n'aient pas accès aux données en question. Le principe de sécurité s'impose au secteur privé comme aux organes fédéraux et les exigences de sécurité doivent également être observées par le mandataire à qui tout ou partie du traitement est délégué[215].

291 La question de la collaboration avec des tiers fait l'objet de dispositions éparses. On relèvera spécialement les dispositions suivantes.

292 <u>*Loi sur la protection des données (LPD)* :</u> La LPD définit les notions de responsable de traitement (« *Verantwortlicher* » ; aussi appelé « *Controller* ») (la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles [art. 5 let. j LPD]) et de sous-traitant (« *Auftragsbearbeiter* » ; aussi appelé « *Processor* ») (la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement [art. 5 let. k LPD]). Le législateur souhaitait se conformer aux nouveaux standards

[212] ANJA MARTINA JOSURAN-BINDER, in: Bieri/Powell (éd.), DSG Kommentar, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023, Art. 40 N 7.
[213] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2836.
[214] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2836.
[215] SYLVAIN MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019 p. 609, 610.

européens[216]. L'allocation de la qualité de responsable du traitement, respectivement de sous-traitant, dépend des circonstances de faits et n'est pas à la libre disposition des parties[217].

293 Autrement dit, lorsqu'il existe un transfert de données personnelles, on peut se trouver en présence i) de deux responsables de traitement indépendants (« *Controller to Controller* »)[218] ; ii) de deux responsables de traitement conjoints (« *Joint Controllers* »)[219] ; ou iii) d'un responsable de traitement et d'un sous-traitant (« *Controller to Processor* »). La question est cruciale[220], mais n'est pas toujours évidente à trancher dans le cas d'espèce[221].

294 En particulier, le prestataire de services qui a certes accès à des données personnelles, mais qui ne font pas l'objet de sa prestation, n'intervient pas comme sous-traitant au sens de la LPD. La simple prise de connaissance, voire la simple possibilité de prendre connaissance de données personnelles ne constitue pas encore un traitement[222]. Un cas de sous-traitance peut néanmoins avoir lieu dans le cadre d'un service de maintenance et d'assistance ; c'est le cas lorsque la prestation comprend également le traitement des données du client pour ce dernier[223].

295 Le responsable du traitement et le sous-traitant sont certes soumis tous deux à des obligations parfois identiques (cf. p. ex. art. 8 LPD, qui prévoit des obligations directes aussi bien à l'égard du responsable du traitement qu'à l'égard du sous-traitant[224]).

296 Cela étant, lorsqu'elle doit être qualifiée de sous-traitance, la collaboration avec un tiers est spécialement régie par l'art. 9 LPD, qui correspond en substance à l'ancien droit (art. 10*a* aLPD, intitulé « Traitement de données par un tiers »[225], qui reprenait l'art. 14 aLPD, anciennement applicable uniquement au traitement de données par des personnes privées[226]). Selon cette disposition, le traitement de données personnelles peut être confié à un sous-traitant pour autant (i) qu'un contrat ou la loi le prévoie et (ii) que les conditions suivantes soient réunies: a) seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui-même; b) aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

297 A l'instar des art. 14 et 10*a* aLPD, l'art. 9 LPD impose au responsable du traitement qui souhaite recourir aux services d'un sous-traitant le devoir de respecter les trois *curae* inspirées de l'art. 55 CO : (i) choisir avec soin le sous-traitant auquel il confie le traitement de données personnelles (*cura in eligendo*), (ii) lui

---

[216] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6643.
[217] EMILIE JACOT-GUILLARMOD, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 59 ad art. 5 LPD.
[218] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17 juin 2019 N 58.
[219] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17 juin 2019 N 58.
[220] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17 juin 2019.
[221] Voir European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, 2 septembre 2020, Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice.
[222] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17 juin 2019 N 96 et 100.
[223] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17 juin 2019 N 103.
[224] EMILIE JACOT-GUILLARMOD, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 3 ad art. 9 LPD.
[225] OFJ, Révision totale de la loi fédérale sur la protection des données (LPD) Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux, octobre 2022, p. 32.
[226] L'art. 14 aLPD ne s'appliquait à l'origine qu'au traitement des données par des *personnes privées*. L'aLPD ne contenait pas de disposition semblable pour le traitement des données par des *organes fédéraux*. Avec son transfert dans la partie générale (art. 10a aLPD), la règle est devenue applicable non seulement aux personnes privées, mais aussi aux organes fédéraux (Message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données du 19 février 2003, FF 2003 1915 1947).

donner toutes les instructions adéquates pour l'accomplissement de son mandat (*cura in instruendo*) et (iii) exercer dans la mesure du possible la surveillance nécessaire (*cura in custodiendo*)[227].

298 La sous-traitance ne dégage pas le responsable du traitement de ses obligations en matière de protection des données[228]. Celui-ci doit s'assurer activement — par le biais d'un choix judicieux du sous-traitant, des instructions données et du contrôle effectué (audits de la sécurité auprès du fournisseur[229]) — que les travaux sont effectués en conformité avec les exigences légales (en particulier en matière de sécurité des données), comme s'il s'en chargeait lui-même. L'externalisation du traitement des données ne doit pas altérer la position juridique de la personne concernée[230].

299 Selon le Message d'ailleurs, l'art. 9 al. 1 LPD « *institue un devoir de diligence à la charge du responsable du traitement, dans le but de sauvegarder les droits des personnes concernées en cas de sous-traitance. Le responsable du traitement doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. Cela concerne principalement le respect des principes généraux de protection des données, les règles relatives à la sécurité – expressément mentionnées à l'al. 2 – ainsi que les règles sur la communication transfrontière. Le responsable du traitement doit, par analogie avec l'art. 55 CO, mettre tout en œuvre pour éviter d'éventuelles violations de la LPD. Il doit ainsi veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire* »[231].

300 En outre, pour recourir à un sous-traitant qui traite des données hors de Suisse, le responsable doit respecter non seulement les exigences relatives à la sous-traitance (art. 9 LPD), mais également celles se rapportant à la communication de données à l'étranger (art. 16 ss LPD)[232], impliquant au besoin l'usage de clauses contractuelles types[233].

301 *Loi sur la sécurité de l'information (LSI)*. Lorsque les autorités et organisations soumises à la LSI collaborent avec des tiers, elles veillent à ce que les exigences et mesures prévues par la LSI soient reprises dans les accords et les contrats qu'elles concluent à cet effet (art. 9 al. 1 LSI). Elles veillent à ce que la mise en œuvre des mesures soit contrôlée de manière adéquate (art. 9 al. 2 LSI).

302 Le Message rappelle que les autorités fédérales ont souvent besoin de l'appui des acteurs de l'économie privée ou d'autres organes pour accomplir leurs tâches. Dans ces cas, les autorités et organisations qui attribuent des mandats à des tiers doivent veiller à ce que les mesures prévues par la loi soient respectées lors de l'attribution et de l'exécution des mandats. Les fournisseurs externes de prestations sont considérés comme des tiers au sens de l'art. 9 LSI et doivent être tenus contractuellement de respecter les mesures prévues par la LSI[234]. En principe, les tiers ne devraient être habilités à accéder aux informations ou aux moyens informatiques de la Confédération que lorsque les mesures de sécurité

---

[227] Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421 470 ; Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6651 ; voir également, parmi d'autres : PHILIPPE MEIER, Protection des données, 2011, par. 1217 s.

[228] OFJ, Révision totale de la loi fédérale sur la protection des données (LPD) Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux, octobre 2022, p. 31.

[229] SYLVAIN MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019 p. 609, 617.

[230] OFJ, Révision totale de la loi fédérale sur la protection des données (LPD) Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux, octobre 2022, p. 31.

[231] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6651.

[232] OFJ, Révision totale de la loi fédérale sur la protection des données (LPD) Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux, octobre 2022, p. 31.

[233] TEO GENECAND, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 57 s. ad art. 16 LPD.

[234] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765 2840 s.

nécessaires ont été mises en œuvre. La LSI contraint également les autorités et organisations soumises à la loi à contrôler de manière adéquate (c'est-à-dire en tenant compte des risques) l'application effective de telles mesures, par exemple en procédant à une visite des lieux ou en demandant une confirmation écrite de la tierce partie[235].

303 De plus, lorsque le mandat implique l'exercice d'une activité sensible, ces autorités et organisations doivent demander l'ouverture d'une procédure de contrôle de sécurité relatif aux personnes (CSP ; cf. art. 27 ss LSI) ou, le cas échéant, d'une procédure de sécurité relative aux entreprises (PSE ; (cf. art. 49 ss LSI)[236].

304 L'art. 10 OSI, qui précise l'art. 9 LSI, prévoit que les unités administratives concernées évaluent les risques pour leurs objets à protéger lors de la collaboration avec des tiers et leur dépendance vis-à-vis de tiers (al. 1). De plus, les services d'achat visés aux art. 9 et 10 de l'ordonnance du 24 octobre 2012 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP) collaborent à l'évaluation et mettent les informations nécessaires à disposition (al. 2).

305 Si la collaboration avec un tiers implique l'accès par ce tiers à des informations, des moyens informatiques, des locaux ou d'autres infrastructures de la Confédération, l'art. 20 LSI prévoit que les autorités et organisations soumises à la LSI veillent à ce que ce tiers (i) soit choisi avec soin, (ii) soit identifié en fonction de la sensibilité de l'activité concernée, (iii) reçoive une formation et une formation continue adaptées à son niveau de responsabilité et (iv) soit le cas échéant tenu au maintien du secret.

306 *Ordonnance sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération (OTUIC)*[237]. En particulier, au sujet du traitement lié à des travaux techniques, les personnes chargées de travaux techniques tels que la maintenance et la gestion de l'infrastructure électronique ne peuvent traiter les données que si l'accomplissement de ces travaux l'exige. La conservation sécurisée des données, leur protection contre les accès illicites et leur confidentialité doivent être préservées (art. 7 al. 1 et 2 OTUIC).

307 *Ordonnance sur la transformation numérique et l'informatique (OTNI)*. Cette ordonnance s'applique en particulier aux unités de l'administration fédérale centrale (art. 2 al. 1 OTNI). En matière de fourniture de prestations et pour ce qui est de la décision relative à l'acquisition de celles-ci, en principe, les départements et la Chancellerie fédérale décident, sur la base d'analyses de marché et en tenant compte des principes d'adéquation, d'interopérabilité, de rentabilité et de sécurité et des exigences en matière de sécurité si les prestations sont fournies par un fournisseur interne ou si elles sont acquises à l'extérieur (art. 8 OTNI).

308 La question de l'accès aux données pour les fournisseurs externes de prestations est réglée spécialement : ils peuvent obtenir l'accès à des données qui ne sont pas accessibles au public si les conditions suivantes sont réunies: a) cet accès est nécessaire pour fournir une prestation; b) l'autorité responsable des données a donné son accord par écrit; c) des mesures contractuelles, organisationnelles et techniques appropriées ont été prises pour éviter que les données soient accessibles à des tiers (« *um eine weitere Verbreitung der Daten zu verhindern* ») (art. 11 al. 1 OTNI). Si l'autorité responsable des données donne elle-même l'accès aux données, il incombe à l'échelon hiérarchique supérieur de donner l'accord prévu à l'al. 1, let. b (art. 11 al. 2 OTNI).

[235] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2831.
[236] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2831.
[237] Basée sur l'art. 57*q* al. 1 LOGA et entrée en vigueur le 1er avril 2012 (RO 2012 947).

(viii) *Ressources appropriées en matière de sécurité de l'information*

309 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités administratives concernées confient des tâches à leurs préposés à la sécurité de l'information et s'assurent notamment qu'ils disposent des compétences et des ressources appropriées (art. 36 al. 4 let. a OSI).

2. Appréciation des cas d'espèce

310 L'analyse juridique des cas de transmission de données vers Xplain implique incidemment de mentionner des comportements adoptés par des employés de la Confédération, d'anciens employés de la Confédération ou par des employés de Xplain. Cela dit, la présente enquête administrative n'est pas une enquête disciplinaire. L'examen de normes pénales ne fait pas non plus partie du mandat de l'Organe d'enquête[238]. Dans ces conditions, les paragraphes qui suivent ne sauraient être interprétés comme une appréciation des faits sous l'angle du droit disciplinaire ou du droit pénal et, par définition, ne lient pas les autorités chargées de leur application.

311 Il va également de soi que les appréciations faites par l'Organe d'enquête au sujet de la protection des données ne lient pas le PFPDT[239].

312 Aucune des normes pertinentes en l'espèce ne contient de conditions subjectives à son application. Déterminer ce que savaient et voulaient les personnes dont le comportement est décrit dans les paragraphes qui suivent n'est donc ni nécessaire, ni pertinent dans le cadre de la présente enquête administrative.

a) Cas de forward n° 1 : un tableur Excel (extraction ORMA) contenant des détails sur des enquêtes pénales et des procédures d'entraide pénale (fedpol) (16 septembre 2020)

313 Ce cas doit faire l'objet d'une analyse sous l'angle de l'aLSIP, de l'aOIAF, de l'aOPrI et de l'aLPD dans leur teneur en vigueur en septembre 2020.

(i) *Normes spéciales applicables à ORMA*

314 ORMA reposait, et repose, sur l'art. 18 de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP ; RS 361)[240]. Selon l'art. 18 al. 1 et 2 aLSIP (dans sa teneur en septembre 2020), Fedpol exploite le système informatisé de gestion interne des affaires et des dossiers, qui peut contenir des données sensibles et des profils de la personnalité. Toutes les communications (retranscriptions ou enregistrements d'appels téléphoniques, courriels, lettres, télécopies) adressées à fedpol ou émanant de cet office peuvent y être saisies. Le système a pour but de traiter les données relatives aux dossiers de fedpol, de gérer l'organisation de manière efficace et rationnelle, d'assurer le suivi des dossiers et d'établir des statistiques.

315 Selon l'art. 3 al. 2, seconde phrase, LSIP, « *[l]es données personnelles peuvent être traitées dans la mesure où elles s'avèrent nécessaires à l'exécution de tâches légales* ».

316 Le fichier Excel « [redacted].xlsx » contient à l'évidence des données personnelles. L'envoi de ce fichier par e-mail au collaborateur de Xplain, à son adresse [Q]@fedpol.admin.ch, constitue *prima facie* un traitement de données qui n'apparait pas nécessaire à l'exécution de tâches légales incombant à fedpol. A notre sens, cet envoi n'apparaît donc pas compatible avec la LSIP.

---

[238] Voir ch. 2.2.2 de la demande d'offres, auquel renvoie le contrat de mandat (AUD B01.01.04.87).
[239] Art. 43 al. 4 LPD.
[240] AUD B03.04.01.10.13.

317 Au surplus, Xplain ne semble entrer dans aucune des catégories de destinataires auxquels fedpol pouvait communiquer des données ORMA aux conditions fixées par l'ordonnance sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (Ordonnance IPAS ; RS 361.2 ; teneur en septembre 2020), applicable à ORMA[241] et par l'Ordonnance sur le système informatisé de la Police judiciaire fédérale (Ordonnance JANUS[242] ; RS 360.2 ; teneur en septembre 2020), également applicable à ORMA[243].

(ii) *Sécurité de l'information*

318 L'art. 26*a* aOIAF entré en vigueur le 1er novembre 2016[244], dont le contenu a été repris par l'art. 11 OTNI, précisait les conditions auxquelles les fournisseurs externes peuvent obtenir l'accès à des données qui ne sont pas accessibles au public : (i) nécessité de l'accès, (ii) accord écrit de l'autorité responsable et (iii) mise en place de mesures contractuelles, organisationnelles et techniques pour éviter l'accès par des tiers.

319 L'art. 12 de l'Ordonnance IPAS (teneur en septembre 2020) renvoyait à l'aOIAF concernant la sécurité « des données ». Il en allait de même de l'art. 29w de l'Ordonnance JANUS (teneur en septembre 2020).

320 Les données contenues dans le fichier Excel en cause sont relatives à des procédures d'enquêtes pénales et des procédures d'entraide judiciaire en matière pénale, lesquelles ne sont pas accessibles au public. L'accès à ces données par Xplain en tant que fournisseur externe supposait donc le respect des conditions de l'art. 26*a* aOIAF.

321 Au vu du contexte, ainsi que du volume et de la nature des données en cause, il est à notre sens d'emblée exclu que leur envoi par e-mail par l'employé de fedpol à l'employé de Xplain – y compris à son adresse e-mail de la Confédération – ait été *nécessaire* au sens de l'art. 26*a* aOIAF.

322 En effet, le problème rencontré par des employés de fedpol dans le cas d'espèce était le suivant : lors de l'extraction de données ORMA vers un tableur Excel, certaines colonnes du tableur restaient vides. Dans son e-mail à l'employé de Xplain, l'employé de fedpol liste les colonnes en question et donne leur descriptif (notamment : ASSERVATEN_NR, SERIEN_NR., VASS_BESCHREIBUNG, ASSERVAT_OERTLICHKEIT etc.).

323 L'Organe d'enquête ne s'explique pas la nécessité d'envoyer par e-mail le tableur Excel lui-même dans ce contexte. Si, par impossible, il existait une nécessité technique d'envoyer le tableur Excel pour permettre à Xplain de régler le problème rencontré avec ORMA, il serait alors inexplicable d'avoir procédé à cet envoi sans supprimer au préalable les données productives contenues de la ligne n° 2 à la ligne n° 39'938. La sélection et la suppression ne prennent pas plus de quelques secondes. A vouloir laisser quelque contenu à titre exemplatif dans le tableur – contre toute nécessité apparente –, il eût été aisé de conserver uniquement une ou deux lignes après avoir pseudonymisé les données qu'elles contenaient.

324 Il est ainsi superflu d'examiner si l'autorité responsable avait donné son accord écrit à l'accès par Xplain ou si des mesures avaient été mises en place pour éviter l'accès par des tiers aux données remises à Xplain.

---

[241] Art. 1 al. 2 let. c Ordonnance IPAS dans sa teneur en septembre 2020.
[242] Aujourd'hui : Ordonnance sur le Système national d'enquête (Ordonnance SNE).
[243] Art. 1 al. 2 let. d Ordonnance JANUS dans sa teneur en septembre 2020. Cf. e-mail de la division juridique de fedpol du 21 février 2019 (AUD 03.10.09.211-215).
[244] RO 2016 3445.

325 En résumé, à notre sens, l'envoi par e-mail du fichier « [redacted].zip » à un employé de Xplain à son adresse [Q]@fedpol.admin.ch n'apparaît pas conforme à l'aOIAF en vigueur au moment des faits.

(iii) *Classification des informations*

326 D'après la classification adoptée par fedpol, les informations contenues dans ORMA relevaient de l'échelon « CONFIDENTIEL » au sens de l'art. 6 aOPrl dans sa teneur en septembre 2020[245].

327 Selon l'art. 13 al. 1 et 2 aOPrl dans sa teneur en septembre 2020, « *[l]'établissement d'informations classifiées, leur communication et le fait de les rendre accessibles doivent être limités à un strict minimum; à cet égard, la situation, la mission, l'objectif et le temps doivent être pris en considération. Il n'est permis de communiquer ou de rendre accessibles des informations classifiées qu'aux personnes qui doivent en avoir connaissance.* »

328 Comme exposé plus haut (cf. *supra* par. 321-323), il n'existait à notre sens aucune nécessité de communiquer les informations contenues dans le fichier Excel en question à Xplain, soit un fournisseur externe, dans le contexte en question.

329 Par conséquent, à notre sens, l'envoi par e-mail du fichier « [redacted].zip » à un employé de Xplain à son adresse [Q]@fedpol.admin.ch n'apparaît pas conforme à l'aOPrl en vigueur au moment des faits.

330 Le fait que le fichier Excel ne contienne pas la mention "CONFIDENTIEL" apparaît en outre incompatible avec les prescriptions de l'aOPrl.

(iv) *Protection des données*

331 Selon notre analyse, les données d'ORMA, système reposant sur l'art. 18 aLSIP, n'entrent pas dans l'exception de l'art. 2 al. 2 let. c aLPD (dans sa teneur en septembre 2020). Formulé positivement, la aLPD s'appliquait, et la LPD s'applique actuellement, au système ORMA de fedpol.

332 Le fichier Excel [redacted]xlsx » contient à l'évidence des données personnelles (sensibles)[246]. Fedpol doit être qualifié de « maître du fichier » au sens de la aLPD (c'est-à-dire « responsable du traitement » selon la terminologie de la LPD).

333 Comme exposé plus haut (cf. *supra* par. 321-323), il n'existait à notre sens aucune nécessité de communiquer les informations contenues dans le fichier Excel en question à Xplain, soit un fournisseur externe, dans le contexte en question.

334 Xplain ne procède à aucun traitement de données personnelles. Certes, Xplain a la possibilité de prendre connaissance des données personnelles (sensibles) figurant dans le fichier Excel. Toutefois, la prestation de Xplain consiste à rédiger un script qui puisse ensuite être utilisé dans ORMA (production), de sorte à ce que, lors d'une prochaine extraction vers Excel, les colonnes signalées par l'employé de fedpol contiennent désormais les données qui devraient s'y trouver. Ce script contient des informations purement techniques ; il ne contient aucune donnée personnelle[247]. Xplain ne peut donc pas, dans le cas d'espèce, être qualifié de sous-traitant de fedpol.

335 A notre sens, l'envoi par e-mail de ce fichier Excel à l'employé de Xplain à son adresse [Q]@fedpol.admin.ch est ainsi susceptible de constituer un traitement non autorisé au sens de l'art. 7

[245] Cf. [redacted]pdf (29.08.2016) (AUD 03.10.09.179).
[246] Données personnelles sur des poursuites ou sanctions pénales (art. 3 let. c ch. 4 aLPD ; art. 5 let. c ch. 5 LPD).
[247] Cf. *supra* par. 81.

aLPD, qui viole *prima facie* l'art. 12 al. 2 let. a aLPD, dans sa teneur en septembre 2020. Aucun des motifs justificatifs de l'art. 13 aLPD ne nous paraît donné en l'espèce[248].

336 Quant à l'art. 7 OTUIC, dont la teneur n'a pas évolué depuis son entrée en vigueur en 2012, et pour autant qu'il soit applicable (il est intitulé : « [redacted] »), il n'autorise un traitement lié à des travaux techniques que si l'accomplissement de ces travaux *l'exige* (art. 7 al. 1 OTUIC). Or, nous avons vu que l'envoi à Xplain des données personnelles (sensibles) figurant dans le fichier Excel n'est pas nécessaire en l'espèce. Cette disposition est donc potentiellement également violée.

(v) *Déficiences en matière technique, d'organisation ou de processus*

337 Il s'agit désormais d'examiner les ordonnances administratives pertinentes en l'espèce et l'existence d'éventuelles déficiences en matière technique, d'organisation ou de processus.

Ordonnances administratives identifiées

338 Parmi les documents qui lui ont été remis, OA a identifié l'ordonnance administrative du DFJP suivante (entrée en vigueur le 01.03.2018) : « Richtlinie für die IKT-Sicherheit im EJPD (EJPD IKT-Richtlinie Sicherheit) ».

339 Ce document indique sous section 3.7 (« Externe Datenverarbeitung ») : « *Die Bearbeitung von geschäftlichen Informationen auf nicht bundeseigenen IKT-Systemen ist nur aufgrund einer vertraglichen Regelung zulässig, welche die sicherheitsrelevanten Belange regelt (IKT-Grundschutz 4.1.3) . Für Externe ist dies vertraglich zu regeln* »[249]. Le document mentionne aussi que « *[e]s dürfen keine Informationen an Unberechtigte weitergegeben werden* »[250].

340 Autrement dit, ce document prévoit que les informations opérationnelles (« *geschäftliche* ») du DFJP ne peuvent être traitées sur un système informatique externe à la Confédération qu'à la condition que (i) cela soit prévu par contrat et que (ii) ce contrat impose des exigences en matière de sécurité informatique. En substance donc, ce texte ne reprend qu'une partie du contenu des dispositions en matière de sécurité de l'information (art. 26*a* aOIAF) et de protection des données (art. 7 al. 1 aLPD) discutées ci-dessus, en particulier l'exigence de mise en place de mesures techniques et contractuelles pour éviter l'accès par des tiers.

341 S'agissant de fedpol en particulier, un autre document intitulé « IT Security – Handbuch Informatiksicherheit fedpol.ch », daté du 01.02.2003, indique ce qui suit : « *Die Wartung aller Informatik-Systeme des Amtes erfolgt durch den Leistungserbringer ISC-EJPD. Soweit Komponenten vor Ort gewartet werden, sind die Aktionen des externen Dienstleisters zu beaufsichtigen. Vor Weitergabe von Geräten an Externe, sind Informationen des Amts auf diesen zu löschen. Sofern die Informationen nicht vollständig gelöscht werden können, ist der externe Dienstleister vertraglich zur Geheimhaltung zu verpflichten mit dem Hinweis auf zivil-, verwaltungs- und strafrechtliche Konsequenzen bei Verletzung dieser Pflicht* »[251].

342 On déduit de ce texte que des données officielles (« *Informationen des Amts* ») ne devraient pas être transférées à des tiers. Si elles le sont néanmoins, il convient de soumettre les prestataires tiers à une obligation de confidentialité. Ce texte reprend ainsi en partie le contenu des dispositions en matière de

[248] Lorsqu'il sollicite l'assistance de ce fournisseur externe, fedpol « agit selon le droit privé » au sens de l'art. 23 aLPD (art. 40 LPD). fedpol était donc soumis aux dispositions de la aLPD applicables aux personnes privées et non à celles applicables aux organes fédéraux. Dans cette mesure, l'exigence de la base légale ne s'applique pas ici (art. 17 al. 1 aLPD applicable aux organes fédéraux).
[249] AUD B03.04.11.10.
[250] AUD B03.04.11.12.
[251] AUD-B03.04.10ter.10.

sécurité de l'information (art. 26*a* aOIAF) et de protection des données (art. 7 al. 1 aLPD) discutées ci-dessus, en particulier l'exigence de mise en place de mesures techniques et contractuelles pour éviter l'accès par des tiers.

343 Cette ordonnance précise également que : « *der Zugang zu Informatik-Systemen und der Zugriff auf Informatik-Anwendungen und Informationen wird stets nur in dem Umfang gewährt, der für die Aufgabenerfüllung erforderlich ist. Gleichermassen ist jeder Mitarbeiter gefordert, den Zugang zu Informatik-Systemen und Zugriff auf Prozesse oder Informationen unberechtigten Dritten zu verwehren. Die Verarbeitung personenbezogener Daten ist nur im festgelegten, gesetzlichen Rahmen zulässig. Eine Nutzung ausserhalb des rechtlichen Rahmens oder die Weitergabe in logischer oder physischer Form ist untersagt* »[252].

344 Par ailleurs, une autre ordonnance administrative intitulée « *Weisung des Direktors betreffend Informationssicherheit fedpol* » du 01.01.2012 précise ce qui suit :

> *« Um Risiken beim Einsatz von E-Mail zu minimieren, gelten folgende Regelungen:*
>
> *- Das Umleiten der persönlichen Mailbox an eine bundesfremde (nicht admin.ch) E Mail-Adresse (z.B. während den Ferien, Geschäftsreisen usw.) ist untersagt.*
>
> *- Das Verwenden von unverschlüsselten E-Mail-Diensten des Internets für den Transfer von dienstlichen Dokumenten oder von Personendaten zur und von der persönlichen Mailbox im EJPD ist verboten (z.B. das Übermitteln von Dokumenten, an denen man zu Hause weiterarbeiten möchte).*
>
> *- Klassifizierte Informationen und datenschutzrechtlich geschützte Personendaten dürfen auf elektronischem Weg nur verschlüsselt übermittelt werden »[253].*

345 Il ressort de cette ordonnance que la redirection d'e-mails d'une adresse personnelle de la Confédération vers une adresse étrangère à la Confédération (« *bundesfremd* ») est expressément interdite. Par ailleurs, il est interdit de transférer des documents officiels (« *dienstlichen Dokumenten* ») et des données personnelles par e-mail non chiffré depuis ou vers l'adresse e-mail personnelle de la Confédération. Enfin, toute communication électronique de données classifiées ou de données personnelles doit être chiffrée.

346 Toutefois, cette ordonnance a été abrogée par la « *Weisung des Direktors betreffend Informationssicherheit fedpol* » du 01.08.2013, laquelle ne contenait plus la section susmentionnée[254].

Appréciation en l'espèce

347 L'impression d'ensemble qui se dégage de l'analyse des ordonnances administratives précitées n'est pas celle de la clarté et de la concision. Ces textes reprennent dans une large mesure les lois et ordonnances applicables, mais n'en respectent pas toujours la terminologie, ce qui est susceptible de causer incertitude ou confusion. A titre d'exemple, on peut se demander qui sont les *Unberechtigte* visés par la Richtlinie für die IKT-Sicherheit im EJPD. Un toilettage, dans le sens d'une réduction des redondances et d'une harmonisation de la terminologie, apparaît ainsi nécessaire[255].

348 Les ordonnances administratives qui nous ont été remises présentent, à notre sens, le défaut de ne pas contenir une interdiction claire de transférer des données productives à des fournisseurs externes,

[252] AUD-B03.04.10ter.13.
[253] AUD-B03.04.10.1248.
[254] AUD-B03.04.10.1242-1245.
[255] Voir les recommandations au terme du rapport (*infra* chapitre VI.B).

accompagnée de règles claires et restrictives sur les accès *on premises* ou *remote* par des fournisseurs externes à des données productives[256].

349 D'une part, le fait que l'employé de fedpol ait envoyé par e-mail ce fichier Excel à l'employé de Xplain en septembre 2020 et, d'autre part, le fait que le fichier en question soit parvenu sur le darknet à la suite de la fuite de données de juin 2023 mettent également en lumière l'insuffisance des mesures prises par fedpol pour se prémunir contre un accès à ses données par des tiers[257].

350 Sur le premier aspect (envoi par l'employé de fedpol à l'adresse [Q]@fedpol.admin.ch), l'employé de fedpol (« A ») a été en mesure (i) d'extraire les données du système ORMA production et (ii) d'envoyer par e-mail à un employé de Xplain, à l'adresse [Q]@fedpol.admin.ch, un fichier compressé de 8 Mo contenant un fichier Excel portant le nom du système ORMA et contenant 39'938 lignes de données extraites de ce système de production. L'enquête n'a identifié ni processus (p. ex. : libération de l'e-mail par un autre employé de fedpol), ni mesure technique (p. ex : blocage automatique de l'envoi d'e-mails qui remplissent certains critères prédéfinis), appliqués avant cet envoi.

351 Le fait que cet employé de fedpol ait procédé à cette extraction et cet envoi par e-mail à un employé de Xplain est également un indice fort que les mesures organisationnelles prises par fedpol en termes de formation et de sensibilisation des personnes traitant des données productives d'ORMA étaient insuffisantes.

352 En outre, il manquait à notre sens des mesures organisationnelles ou techniques pour que le fait que Q était un employé d'un fournisseur externe soit immédiatement reconnaissable pour tout employé de la Confédération entrant en contact avec Q : à titre d'exemple, l'adresse e-mail [Q]@fedpol.admin.ch aurait pu contenir une mention « externe » ou similaire. Il est par ailleurs problématique que la signature automatique figurant au pied de l'e-mail de l'employé de Xplain donne l'impression qu'il est un employé de fedpol.

353 Sous l'angle technique, nous relevons également qu'au moment de l'extraction vers Excel, le système n'a pas apposé automatiquement une mention « CONFIDENTIEL » alors que les données extraites de ORMA production étaient classifiées comme tel.

354 Quant au second aspect (présence du fichier dans l'environnement informatique de Xplain et *in fine* sur le darknet), l'employé de Xplain a ensuite été en mesure d'envoyer ce même fichier depuis son adresse [Q]@fedpol.admin.ch vers son adresse [Q]@xplain.ch. Ici aussi, l'enquête n'a identifié ni processus, ni mesure technique, appliqués avant cet envoi.

355 Xplain devait, selon les conditions générales de la Confédération intégrées dans les contrats avec fedpol, prendre toutes les mesures que l'on pouvait raisonnablement attendre d'elle du point de vue économique et toutes les mesures techniques et organisationnelles possibles, de manière que les données produites et échangées dans le cadre de l'exécution du contrat ne parviennent pas à la connaissance de tiers non autorisés. Cette mesure contractuelle est nécessaire mais non suffisante. En l'espèce:

i. Aucune mesure concrète n'était contractuellement exigée de Xplain.

ii. Nous n'avons identifié aucun contrôle par fedpol du respect de cette obligation.

[256] Voir les recommandations au terme du rapport (*infra* chapitre VI.B).
[257] Voir les recommandations au terme du rapport (*infra* chapitre VI.B).

356 Plusieurs personnes interrogées ont relevé que les employés de Xplain avaient passé avec succès un contrôle de sécurité lié aux personnes (CSP). C'était notamment le cas de Q.

357 Toutefois, le CSP permet une prise de vue du passé à un instant T et ne couvre pas le futur, jusqu'à ce qu'il soit renouvelé dans les délais fixés par l'ordonnance. Historiquement, le CSP avait essentiellement pour but, aux termes de la LMSI, de répondre aux besoins de protection des informations dans le domaine de la sûreté intérieure ou extérieure de la Confédération, même si les ordonnances ont ensuite étendu sa portée[258]. En substance, le Service spécialisé chargé d'effectuer le contrôle consultait essentiellement des registres de données judiciaires et de police, le cas échéant sollicitait l'assistance d'Etats étranger lorsqu'un accord le permettait. Pour certaines catégories de personnes, le Service auditionnait en outre la personne soumise au contrôle (« Contrôle de sécurité élargi avec audition »). En l'occurrence et à notre connaissance, aucun des employés de Xplain n'a fait l'objet de ce contrôle élargi avec audition.

358 De tels contrôles nous paraissent nécessaires, mais non suffisants, pour s'assurer qu'une personne dispose de la sensibilité nécessaire dans le domaine de la sécurité de l'information.

359 En outre, le CSP ne visait que les personnes physiques et ne renseignait pas sur la sécurité de l'information de l'entreprise avec laquelle la Confédération entrait ou était en relation contractuelle[259]. A cet égard, l'OCSCP en vigueur au moment des faits prévoyait la possibilité de soumettre une entreprise externe à la Confédération ayant accès à des informations classifiées CONFIDENTIEL ou SECRET de la Confédération à une procédure de « maintien du secret » (« *Betriebssicherheitserklärung ; BSE* »). L'enquête n'a identifié aucune déclaration « BSE » relative à Xplain. Un échange interne d'e-mails de décembre 2020 tend à confirmer que Xplain ne disposait pas, et n'avait jamais disposé, d'une déclaration « BSE »[260].

360 La déclaration d'engagement signée par l'employé de Xplain vise-t-elle le transfert de données non accessibles au public par cet employé depuis un e-mail de la Confédération vers son adresse e-mail de Xplain ? En particulier, est-ce que le transfert *en dehors des locaux* du mandant (« *ausserhalb Räumlichkeiten des Auftraggebers* ») ne vise que les transferts physiques, comme une interprétation littérale le suggère, ou également le transfert par e-mail, comme une interprétation téléologique l'impose probablement ? Nous constatons ainsi que la déclaration d'engagement signée par l'employé de Xplain laissait trop d'espace à l'interprétation.

361 Enfin, les mesures techniques, contractuelles et organisationnelles présentées ci-dessus sont toutes prises en amont de la relation contractuelle. Or, des mesures prises en cours de relation, comme des contrôles ou des audits, demeurent indispensables, ne serait-ce que pour évaluer le respect des engagements contractuels. De telles mesures n'ont toutefois pas été identifiées en l'espèce.

362 Les recommandations présentées plus bas exposeront les améliorations suggérées afin de prévoir d'autres mesures de protection et de combler les déficiences évoquées.

---

[258] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765, 2796. Voir aussi Message concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire « S. o. S. - pour une Suisse sans police fouineuse » du 7 mars 1994, FF 1994 II 1123, 1145 : « L'une des menaces les plus grandes et les plus vives pour la sûreté intérieure vient des personnes occupant des postes clés qui commettent une trahison, travaillent contre l'Etat lui-même ou veulent changer ses institutions de manière illicite ».

[259] Comparer aujourd'hui avec le contrôle prévu par l'OPSEnt, entrée en vigueur le 1er janvier 2024.

[260] Echange d'e-mails entre l'ISBO d'armasuisse et un chargé de projet d'armasuisse entre le 10 et le 17 décembre 2020 (AUD 03.10.09.257-260).

b) Cas de forward n° 2 : divers fichiers joints à un e-mail, contenant notamment des informations classifiées sur les Conseillers fédéraux et des fonctionnaires étrangers (5 mai 2018)

363 L'analyse ci-dessus (let. a) s'applique pour l'essentiel au présent cas. En substance, celui-ci concerne l'envoi à un employé de Xplain à son adresse [R]@fedpol.admin.ch de documents de fepdol classifiées CONFIDENTIEL, datant de fin 2017 respectivement début 2018, relatifs à des rencontres impliquant des haut-fonctionnaires nationaux et internationaux, ainsi que des informations relatives à des conseillers fédéraux.

364 En résumé, les normes spéciales applicables à ORMA (notamment la LSIP) ainsi que les dispositions en matière de sécurité de l'information (aOIAF) et en matière de classification des informations (aOPrI) apparaissent *prima facie* ne pas avoir été respectées. Le même constat s'applique aux dispositions en matière de protection des données (aLPD).

365 L'examen des déficiences en matière technique, d'organisation ou de processus contribuant à expliquer l'envoi à l'employé de Xplain des documents en cause, en violation des normes examinées dans les sections précédentes, a déjà été exposé ci-dessus, de sorte qu'il convient d'y renvoyer.

c) Cas de forward n° 3 : l'envoi d'un tableur Excel contenant plus de 1'000 lignes relatives à des notices Interpol (1er septembre 2021)

366 En substance, ce concerne un fichier Excel intitulé « [redacted] .xlsx ».

367 Ce fichier compte 1'045 lignes et 32 colonnes contenant des informations relatives à des notices Interpol de différentes catégories. Il contient des données personnelles (sensibles). De toute évidence, ce tableur Excel est le résultat d'une extraction depuis ORMA, système dont le contenu est classifié CONFIDENTIEL.

368 L'enquête n'a pas permis de déterminer si l'employé Xplain (Z) a préalablement reçu d'un employé fedpol le fichier Excel en question ou si Z lui-même a procédé à une extraction de données du système de production ORMA et dans cette hypothèse dans quelles circonstances.

369 Dans la première hypothèse (envoi par un employé fedpol à cet employé Xplain), l'analyse exposée ci-dessus (cf. let. a) est également applicable. La deuxième hypothèse (accès au système de production par l'employé Xplain) est traitée plus bas, de sorte qu'on y renvoie[261].

370 Dans les deux hypothèses et en résumé, les normes spéciales applicables à ORMA (notamment la LSIP) ainsi que les dispositions en matière de sécurité de l'information (aOIAF) et en matière de classification des informations (aOPrI) apparaissent *prima facie* ne pas avoir été respectées. Le même constat s'applique aux dispositions en matière de protection des données (aLPD).

371 Afin d'éviter des répétitions, il peut être renvoyé *mutatis mutandis* à l'analyse des déficiences en matière technique, d'organisation ou de processus qui a été faite dans le premier cas ci-dessus.

d) Cas d'accès : un tableur Excel (extraction ORMA) contenant le « Betreff » des affaires (22 septembre 2011)

372 Ce cas doit faire l'objet d'une analyse sous l'angle de l'aLSIP, de l'aOIAF 2003, de l'aOPrI et de l'aLPD dans leur teneur en vigueur en septembre 2010.

[261] Cf. *infra* V.A.2.d).

(i) *Normes spéciales applicables à ORMA*

373 Les normes spéciales applicables à ORMA ont été exposées ci-dessus (par. 314-315), de sorte qu'on y renvoie.

374 Comme indiqué dans la partie en fait de ce rapport[262], il apparaît que S, qui était alors employé au sein de Xplain, disposait au moment des faits (septembre 2010) d'un accès au système de production ORMA de fedpol. Les modalités exactes dans lesquelles cet accès s'exerçait n'ont pas pu être établies.

375 Cela étant, il apparaît que S a pu, selon toute vraisemblance, extraire des données de ORMA (production) vers un fichier Excel. Dans des circonstances factuelles que l'enquête n'a pas permis de clarifier définitivement, ce fichier Excel s'est trouvé dans l'environnement informatique de Xplain.

376 Enfin, S a envoyé ce fichier par e-mail non chiffré depuis son adresse [S]@xplain.ch à des employés de fedpol à leur adresse @fedpol.admin.ch.

377 Le fichier Excel « [redacted] *.xls* », en particulier sa colonne C intitulée « *Betreff* », contient à l'évidence des données personnelles, y compris des données personnelles sensibles (plus de 8'000 lignes d'informations détaillées relatives à diverses procédures, notamment pénales).

378 L'accès à ces données, leur extraction, leur sauvegarde dans l'environnement informatique d'un fournisseur externe et leur envoi depuis cet environnement par e-mail non chiffré vers l'environnement informatique de fedpol constituent *prima facie* des traitements de données qui n'apparaissent pas nécessaire à l'exécution de tâches légales incombant à fedpol. A notre sens, ces traitements n'apparaissent pas compatibles avec la LSIP.

379 Lors de son interrogatoire, F a déclaré en substance que S n'avait pas besoin des informations qui figuraient dans la colonne C intitulée « *Betreff* » pour réaliser la tâche attendue de lui[263].

380 Au surplus, la cas en cause ne paraît pas entrer dans un cas de figure en vertu duquel un droit d'accès aurait pu être accordé à Xplain sur la base de l'ordonnance sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (Ordonnance IPAS ; RS 361.2 ; teneur en septembre 2010), applicable à ORMA[264], et de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (Ordonnance JANUS[265] ; RS 360.2 ; teneur en septembre 2010), également applicable à ORMA[266] ; Xplain ne semble pas non plus pouvoir entrer dans les catégories de destinataires auxquels fedpol pouvait communiquer des données ORMA en vertu des deux ordonnances précitées.

(ii) *Sécurité de l'information*

381 L'art. 12 de l'Ordonnance IPAS (teneur en septembre 2010) renvoyait, concernant la sécurité « des données », à l'aOIAF 2003 ainsi qu'aux directives du CI du 27 septembre 2004 concernant la sécurité informatique dans l'administration fédérale. Il en allait de même de l'art. 26 de l'Ordonnance JANUS (teneur en septembre 2010).

382 Or, aucun de ces textes ne réglait l'accès aux données par les fournisseurs externes de prestations informatiques.

---

[262] Cf. *supra* par. 101-115.
[263] *Supra* par. 113.
[264] Art. 1 al. 2 let. c Ordonnance IPAS dans sa teneur en septembre 2010.
[265] Aujourd'hui : Ordonnance sur le Système national d'enquête (Ordonnance SNE).
[266] Art. 1 al. 2 let. d Ordonnance JANUS dans sa teneur en septembre 2020. Cf. e-mail de la division juridique de fedpol du 21 février 2019 (AUD 03.10.09.211-215).

383 L'art. 26*a* aOIAF évoqué dans les cas précédents contenait une règle sur l'accès aux données pour les fournisseurs externes de prestations informatiques, mais il est entré en vigueur postérieurement aux faits, à savoir le 1er novembre 2016[267].

(iii) *Classification des informations*

384 D'après la classification adoptée par fedpol, les informations contenues dans ORMA relevaient de l'échelon « CONFIDENTIEL » au sens de l'art. 6 aOPrl dans sa teneur en septembre 2010[268].

385 Selon l'art. 13 al. 1 et 2 aOPrl dans sa teneur en septembre 2010, « *[l]'établissement d'informations classifiées, leur communication et le fait de les rendre accessibles doivent être limités à un strict minimum; à cet égard, la situation, la mission, l'objectif et le temps doivent être pris en considération. Il n'est permis de communiquer ou de rendre accessibles des informations classifiées qu'aux personnes qui doivent en avoir connaissance*. »

386 A notre sens, l'accès à ces données par S, leur extraction, leur sauvegarde dans l'environnement informatique d'un fournisseur externe et leur envoi depuis cet environnement par e-mail non chiffré vers l'environnement informatique de fedpol n'apparaissent pas nécessaires dans le contexte de faits en question. L'aOprl paraît ainsi avoir été violée dans le cas d'espèce.

387 Le fait que la mention "CONFIDENTIEL" ne figure pas sur le fichier Excel en question semble en outre incompatible avec les prescriptions de l'aOPrl.

(iv) *Protection des données*

388 Selon notre analyse, les données d'ORMA, système reposant sur l'art. 18 aLSIP, n'entrent pas dans l'exception de l'art. 2 al. 2 let. c aLPD (dans sa teneur en septembre 2010). Formulé positivement, la aLPD s'appliquait, et la LPD s'applique actuellement, au système ORMA de fedpol.

389 Le fichier Excel « [redacted]*.xls* » contient à l'évidence des données personnelles (sensibles)[269]. Fedpol doit être qualifié de « maître du fichier » au sens de la aLPD (c'est-à-dire « responsable du traitement » selon la terminologie de la LPD).

390 Comme exposé plus haut, dans le contexte en question, il n'existait à notre sens aucune nécessité d'accorder un accès à ORMA (production) à un employé de Xplain, soit un fournisseur externe, qui a permis à cet employé de procéder à une extraction de données personnelles (sensibles) contenues dans ORMA et de les envoyer ensuite, depuis l'environnement informatique de Xplain, à une adresse e-mail @fedpol.ch.

391 De plus, Xplain procède *de facto* à un traitement de données personnelles sur instruction de fedpol. En effet, Xplain extrait des données personnelles (sensibles) de ORMA avant de les envoyer par e-mail à un employé de fedpol conformément aux instructions d'un autre employé de fedpol.

392 A notre sens, Xplain doit donc, dans le cas d'espèce, être qualifié de sous-traitant de fedpol.

---

[267] RO 2016 3445. Le contenu de l'art. 26a aOIAF, qui a été repris par l'art. 11 OTNI, précisait les conditions auxquelles les fournisseurs externes peuvent obtenir l'accès à des données qui ne sont pas accessibles au public, à savoir : (i) nécessité de l'accès, (ii) accord écrit de l'autorité responsable et (iii) mise en place de mesures contractuelles, organisationnelles et techniques pour éviter l'accès par des tiers. Voir également : communiqué du Conseil fédéral du 30 septembre 2016 « Le Conseil fédéral restreint la transmission de données aux prestataires informatiques externes lors de la production et de l'exploitation de systèmes d'information ».

[268] Cf [redacted].pdf (29.08.2016) (AUD 03.10.09.179).

[269] Données personnelles sur des poursuites ou sanctions pénales (art. 3 let. c ch. 4 aLPD ; art. 5 let. c ch. 5 LPD).

393 Or, il résulte de l'enquête que les contrats relatifs à ORMA ne prévoyaient pas, et *a fortiori* n'encadraient pas, la sous-traitance par Xplain. L'exigence centrale posée par l'art. 10a aLPD n'apparait ainsi pas respectée[270].

394 En n'encadrant pas contractuellement ce rapport de sous-traitance, fedpol n'a, *a fortiori,* pas eu de visibilité sur la localisation des traitements et le recours éventuel à des sous-sous-traitants (étant rappelé que Xplain dispose de bureaux à l'étranger exploités par des filiales sises en Espagne et en Allemagne)[271].

395 En définitive, le cas d'espèce consacre *prima facie* des traitements non autorisés au sens de l'art. 7 aLPD, qui violent l'art. 12 al. 2 let. a aLPD, dans sa teneur en septembre 2010. Aucun des motifs justificatifs de l'art. 13 aLPD ne nous paraît donné en l'espèce[272].

(v) *Déficiences en matière technique, d'organisation ou de processus*

396 Il s'agit désormais d'examiner les ordonnances administratives pertinentes en l'espèce et l'existence d'éventuelles déficiences en matière technique, d'organisation ou de processus.

397 Parmi les documents qui lui ont été remis, OA a identifié les ordonnances administratives suivantes :

i. Un document « *Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD (Online-Weisung EJPD)* »[273] du 30 septembre 2004 (entrée en vigueur le 1er octobre 2004), qui règle a) les conditions de mise en place d'une liaison en ligne entre le DFJP et des organes de la Confédération et des cantons, qui permet aux employés de ces organes (utilisateurs) d'avoir accès à une application informatique du DFJP, et b) les conditions d'octroi d'une autorisation d'accès individuelle à ces utilisateurs lorsque des données personnelles leur sont rendues accessibles au moyen de cette liaison en ligne (cf. art. 1 al. 2 de la directive) ; autrement dit, un accès à des utilisateurs hors organes de la Confédération et des cantons n'est pas prévu ;

ii. Un autre document « *Weisung des EJPD über die Umsetzung des Datenschutzes und Informationssicherheit (DSIS-Weisung EJPD)* »[274] du 12 mai 2011 (entrée en vigueur le 1er juin 2011), prévoit (par. 22, sous « *Kontrolle und Berichterstattung*») ce qui suit : « *Die Umsetzung von DSIS wird auf der Stufe Departement und in den Verwaltungseinheiten regelmässig kontrolliert, damit Mängel rechtzeitig erkannt und durch geeignete Massnahmen behoben werden können*. » ;

iii. Un document « *Handbuch Informatiksicherheit* »[275] du 1er février 2003 de fedpol (entrée en vigueur non précisée), qui prévoit ce qui suit (section 4.1.11, intitulée « Wartung ») : « *Die Wartung aller Informatik-Systeme des Amtes erfolgt durch den Leistungserbringer ISC-EJPD. Soweit Komponenten vor Ort gewartet werden, sind die Aktionen des externen Dienstleisters zu beaufsichtigen. Vor Weitergabe von Geräten an Externe, sind Informationen des Amts auf diesen zu löschen. Sofern die Informationen nicht vollständig gelöscht werden können, ist der externe Dienstleiter vertraglich zur Geheimhaltung zu verpflichten mit dem Hinweis auf zivil-, verwaltungs- und strafrechtliche*

[270] Sur la question des trois *curae*, cf. ci-dessous par. 499 ss.
[271] Cf. *supra* par. 214-217.
[272] Lorsqu'il sollicite l'assistance de ce fournisseur externe, fedpol « agit selon le droit privé » au sens de l'art. 23 aLPD (art. 40 LPD). fedpol était donc soumis aux dispositions de la aLPD applicables aux personnes privées et non à celles applicables aux organes fédéraux. Dans cette mesure, l'exigence de la base légale ne s'applique pas ici (art. 17 al. 1 aLPD applicable aux organes fédéraux).
[273] AUD B03.04.10.934-941.
[274] AUD B03.04.10.1185-1194.
[275] AUD B03.04.10ter.1-24.

Konsequenzen bei Verletzung dieser Pflicht. Allenfalls kann zusätzlich eine Konventionalstrafe vereinbart werden. ». De plus, la section 4.3 (« *Sicherheitsleitsätze* ») a la teneur suivante : « *Der Zutritt zu Gebäuden und Räumlichkeiten, der Zugang zu Informatik-Systemen und der Zugriff auf Informatik-Anwendungen und Informationen wird stets nur in dem Umfang gewährt, der für die Aufgabenerfüllung erforderlich ist. Gleichermassen ist jeder Mitarbeiter gefordert, den Zugang zu Informatik-Systemen und Zugriff auf Prozesse oder Informationen unberechtigten Dritten zu verwehren*. » ;

iv. Enfin, un document « *Weisung des Direktors fedpol betreffend Informationsshicherheit fepdol* »[276] du 1er mars 2007 (entrée en vigueur le 1er mars 2007), qui dispose (section 4, « *E-mail* »), que « *Ohne Chiffrierung dürfen generell keine klassifizierten Informationen und keine datenschutzrechtlich geschützten Personendaten elektronisch übermittelt werden, weder innerhalb noch ausserhalb der Bundesverwaltung. Der Versand solcher Informationen muss immer eingeschrieben auf postalischem Weg erfolgen*. »

398 On déduit de ces textes que l'accès à des données personnelles est encadré par des conditions, qui devraient faire l'objet de contrôles réguliers. De plus, l'ISC-DFJP est en charge de la maintenance des systèmes informatiques de fedpol, et on comprend qu'un prestataire de service externe ne doit pas avoir accès à des données officielles (« *Informationen des Amts* »). Celles-ci doivent en principe être effacées sur les appareils qui seraient remis à un prestataire de service externe. Si ces données ne peuvent pas être effacées complètement, ce prestataire doit être soumis à une obligation de confidentialité, avec renvoi aux conséquences civiles, administratives et pénales en cas de violation de cette obligation. Enfin, l'accès accordé à des applications informatiques ne doit être accordé que dans la mesure nécessaire à l'exécution de la tâche ; chaque collaborateur doit refuser l'accès à des systèmes informatiques ou à des informations à des tiers non autorisés.

399 Ces textes reprennent ainsi en partie le contenu des dispositions en matière de protection des données (art. 7 al. 1 aLPD) discutées ci-dessus, en particulier l'exigence de mise en place de mesures destinées à éviter l'accès par des tiers.

400 Afin d'éviter des répétitions, il peut être renvoyé *mutatis mutandis* à l'analyse des déficiences en matière technique, d'organisation ou de processus qui a été faite dans le premier cas ci-dessus.

e) Cas de transfert actif n° 1 : des captures d'écran envoyées dans le cadre de la migration PAGIRUS-TROVA (28 janvier 2016)

401 Ce cas doit faire l'objet d'une analyse sous l'angle de l'aLSIP, de l'aOIAF, de l'aOPrI et de l'aLPD dans leur teneur en vigueur en janvier 2016.

(i) *Normes spéciales applicables à PAGIRUS*

402 PAGIRUS était réglé essentiellement par l'ordonnance sur le système de gestion de personnes, de dossiers et d'affaires (PAGIRUS) de l'Office fédéral de la justice (Ordonnance PAGIRUS)[277] abrogée au 1er novembre 2016[278], puis par l'ordonnance sur le système électronique de gestion de personnes, de dossiers et d'affaires de l'Office fédéral de la justice (Ordonnance GPDA)[279].

[276] AUD B03.04.10bis.1-5.
[277] RO 2010 1.
[278] RO 2016 3261.
[279] RS 351.12.

403 L'ordonnance PAGIRUS reposait sur l'art. 57h al. 2 LOGA, qui prévoyait, au moment des faits, que « *Seuls les collaborateurs de l'organe concerné ont accès à des données personnelles, et uniquement dans la mesure où ces données sont nécessaires à l'accomplissement de leurs tâches*. »

404 Les pièces jointes annexées à l'e-mail du 28 janvier 2016 contiennent à l'évidence des données personnelles. L'envoi de ces pièces par e-mail au collaborateur de Xplain, à son adresse [T]@xplain.ch, constitue un traitement de données qui n'apparait pas nécessaire à l'exécution de tâches légales incombant à l'OFJ. A notre sens, cet envoi n'était donc pas compatible avec l'art. 57h al. 2 LOGA. Il résulte d'ailleurs de l'interrogatoire de G que Xplain n'était pas compétente pour procéder à la migration en tant que telle ; Xplain se chargeait uniquement de fournir le script permettant ensuite le transfert de données d'une application à l'autre. Ainsi, des données anonymisées ou caviardées étaient suffisantes dans le cadre de cette activité de support[280].

405 Au surplus, Xplain n'entrait dans aucune des catégories de destinataires auxquels l'OFJ pouvait communiquer des données PAGIRUS aux conditions fixées par l'ordonnance PAGIRUS.

(ii) *Sécurité de l'information*

406 L'art. 13 al. 1 de l'Ordonnance PAGIRUS renvoyait, concernant la « Sécurité informatique », à l'aOPD, l'aOIAF 2003 ainsi qu'aux directives du CI du 27 septembre 2004 concernant la sécurité informatique dans l'administration fédérale.

407 Or, aucun de ces textes ne réglait l'accès aux données pour les fournisseurs externes de prestations informatique.

408 L'art. 26*a* aOIAF évoqué dans les cas précédents contenait une règle sur l'accès aux données pour les fournisseurs externes de prestations informatiques, mais il est entré en vigueur postérieurement aux faits, à savoir le 1er novembre 2016[281].

409 En outre, l'art. 13 al. 2 de l'Ordonnance PAGIRUS prévoyait que l'OFJ arrête dans le règlement sur le traitement des données visé à l'art. 2, al. 2, les mesures organisationnelles et techniques visant à empêcher le traitement non autorisé des données ; il y définit également les modalités de la journalisation automatique du traitement et de la consultation des données.

(iii) *Protection des données*

410 Selon notre analyse, les données de PAGIRUS n'entrent pas dans l'exception de l'art. 2 al. 2 let. c aLPD (dans sa teneur en janvier 2016). Formulé positivement, la aLPD s'appliquait, et la LPD s'applique actuellement, au système PAGIRUS de l'OFJ.

411 Les pièces envoyées en annexe à l'e-mail en question contiennent à l'évidence des données personnelles (sensibles)[282]. L'OFJ doit être qualifié de « maître du fichier » au sens de la aLPD (c'est-à-dire « responsable du traitement » selon la terminologie de la LPD).

---

[280] Enregistrement audio de l'interrogatoire n° 231128-002.

[281] RO 2016 3445. Le contenu de l'art. 26a aOIAF, qui a été repris par l'art. 11 OTNI, précisait les conditions auxquelles les fournisseurs externes peuvent obtenir l'accès à des données qui ne sont pas accessibles au public, à savoir : (i) nécessité de l'accès, (ii) accord écrit de l'autorité responsable et (iii) mise en place de mesures contractuelles, organisationnelles et techniques pour éviter l'accès par des tiers. Voir également : communiqué du Conseil fédéral du 30 septembre 2016 « Le Conseil fédéral restreint la transmission de données aux prestataires informatiques externes lors de la production et de l'exploitation de systèmes d'information ».

[282] Données personnelles sur des poursuites ou sanctions pénales (art. 3 let. c ch. 4 aLPD ; art. 5 let. c ch. 5 LPD).

412 Comme exposé plus haut, il n'existait à notre sens aucune nécessité de communiquer les informations contenues dans les pièces en question à Xplain, soit un fournisseur externe, ni au consultant externe également en copie, dans le contexte de la migration de données du système PAGIRUS à TROVA.

413 Sur la base des informations à notre disposition, nous déduisons que le rôle de Xplain était limité à une prestation d'assistance dans le cadre d'une migration effectuée par l'OFJ. En ce sens, Xplain ne devrait pas être qualifié de sous-traitant pour cette prestation-là.

414 A notre sens, l'envoi par e-mail de ces fichiers à l'employé de Xplain à son adresse [T]@xplain.ch est ainsi susceptible de constituer un traitement non autorisé au sens de l'art. 7 aLPD, qui viole *prima facie* l'art. 12 al. 2 let. a aLPD, dans sa teneur en janvier 2016. Aucun des motifs justificatifs de l'art. 13 aLPD ne nous paraît donné en l'espèce[283].

415 Quant à l'art. 7 OTUIC, dont la teneur n'a pas évolué depuis son entrée en vigueur en 2012, et pour autant qu'il soit applicable (il est intitulé : « Traitement lié à des travaux techniques »), il n'autorise un traitement lié à des travaux techniques que si l'accomplissement de ces travaux *l'exige* (art. 7 al. 1 OTUIC). Or, nous avons vu que l'envoi à Xplain des données personnelles (sensibles) figurant dans les pièces jointes en cause n'est pas nécessaire en l'espèce. Cette disposition est donc potentiellement également violée.

(iv) *Déficiences en matière technique, d'organisation ou de processus*

416 Il s'agit désormais d'examiner les ordonnances administratives pertinentes en l'espèce et l'existence d'éventuelles déficiences en matière technique, d'organisation ou de processus.

417 Parmi les documents qui lui ont été remis, OA a identifié l'ordonnance administrative suivante applicable au moment des faits (janvier 2016) : « *Weisung des EJPD über die Umsetzung des Datenschutzes und Informationssicherheit (DSIS-Weisung EJPD)* »[284] du 12 mai 2011 (entrée en vigueur le 1er juin 2011) ; elle renvoie aux règles applicables en matière de protection des données, de sécurité de l'information et de protection de l'information (par. 13 à 16). Par ailleurs, elle prévoit (par. 22, sous «*Kontrolle und Berichterstattung*») ce qui suit : « *Die Umsetzung von DSIS wird auf der Stufe Departement und in den Verwaltungseinheiten regelmässig kontrolliert, damit Mängel rechtzeitig erkannt und durch geeignete Massnahmen behoben werden können*. ».

418 On déduit de ce texte que l'accès à des données personnelles est encadré par des conditions, qui devraient faire l'objet de contrôles réguliers. Ces textes reprennent ainsi en partie le contenu des dispositions en matière de protection des données (art. 7 al. 1 aLPD) discutées ci-dessus, en particulier l'exigence de mise en place de mesures destinées à éviter l'accès par des tiers.

419 Afin d'éviter des répétitions, il peut être renvoyé *mutatis mutandis* à l'analyse des déficiences en matière technique, d'organisation ou de processus qui a été faite dans le premier cas ci-dessus.

[283] Lorsqu'il sollicite l'assistance de ce fournisseur externe, l'OFJ « agit selon le droit privé » au sens de l'art. 23 aLPD (art. 40 LPD). L'OFJ était donc soumis aux dispositions de la aLPD applicables aux personnes privées et non à celles applicables aux organes fédéraux. Dans cette mesure, l'exigence de la base légale ne s'applique pas ici (art. 17 al. 1 aLPD applicable aux organes fédéraux).
[284] AUD B03.04.10.1185-1194.

f) Cas de transfert actif n° 2 : un tableur Excel concernant 156 patrouilles de la Police militaire (30 juillet 2020)

(i) *Normes spéciales applicables à JORASYS*

420 Le Système de journal et de rapport de la Police militaire (JORASYS) reposait au moment des faits, et repose toujours, sur les art. 167a ss de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS (LSIA)[285].

421 JORASYS sert à l'accomplissement des tâches visées à l'art. 100 al. 1 LAAM, notamment: a) tenir le journal des centrales d'engagement du commandement de la police militaire; b) établir les rapports sur les tâches de police judiciaire et de police de sûreté des formations professionnelles du commandement de la police militaire; c) apprécier la situation militaire sur le plan de la sécurité; d) assurer l'autoprotection de l'armée (art. 167b LSIA).

422 JORASYS contient des données sur les personnes soumises au droit pénal militaire, relatives à des tiers en lien avec des incidents en rapport avec l'armée ou des militaires (art. 167c LSIA). La communication des données est régie par l'art. 167e LSIA, qui contient une liste de personnes et services autorisés à avoir accès aux données, ou à se voir communiquer des extraits, de JORASYS.

423 Les personnes chargées de la maintenance, de la gestion et de la programmation ne peuvent traiter des données que si elles sont absolument nécessaires à l'accomplissement de leurs tâches et que la sécurité des données est garantie. Il ne doit en résulter aucune modification des données (art. 7 al. 2 LSIA).

424 En l'espèce, le fichier Excel « [redacted] *.xls* »[286] contient à l'évidence des données sur les personnes soumises au droit pénal militaire, provenant, ou plus vraisemblablement destinées, à être intégrées dans JORASYS. L'envoi de ce fichier par e-mail au collaborateur de Xplain sur son adresse [U]@xplain.ch, ainsi qu'à l'adresse de support de Xplain (support@xplain.ch), constitue une communication des données qui n'apparait pas compatible avec l'art.167e LSIA. L'enquête n'a pas pu déterminer quelles personnes physiques recevaient au moment des faits les e-mails adressés à support@xplain.ch.

425 De plus, il apparaît que l'employé de la Police militaire pouvait procéder seul à l'opération en question (ajouter 156 patrouilles dans JORASYS). S'il s'est adressé à la BAC, c'est apparemment afin de gagner de temps.

426 Un incident a été ouvert auprès de la *Hotline* de la BAC, mais cette ouverture semble purement formelle. La BAC a immédiatement transmis le cas à Xplain et n'a, apparemment, effectué aucune autre démarche.

427 A notre sens, l'envoi à Xplain par la BAC n'était donc pas compatible avec la LSIA.

(ii) *Sécurité de l'information*

428 L'art. 26*a* aOIAF entré en vigueur le 1er novembre 2016[287], dont le contenu a été repris par l'art. 11 OTNI, précisait les conditions auxquelles les fournisseurs externes peuvent obtenir l'accès à des données qui ne sont pas accessibles au public : (i) nécessité de l'accès, (ii) accord écrit de l'autorité responsable et (iii) mise en place de mesures contractuelles, organisationnelles et techniques pour éviter l'accès par des tiers.

[285] RS 510.91.
[286] AUD B03.10.05.01.
[287] RO 2016 3445.

429 Les données contenues dans le fichier Excel en cause sont relatives à des patrouilles de la Police miliaire, non accessibles au public. L'accès à ces données par Xplain en tant que fournisseur externe supposait donc le respect des conditions de l'art. 26*a* aOIAF.

430 Au vu du contexte rappelé ci-dessus, nous retenons que leur envoi par e-mail par l'employé de la BAC à l'employé de Xplain n'était pas *nécessaire* au sens de l'art. 26*a* aOIAF. Il apparaît en effet que la Police militaire pouvait procéder seule à l'opération en question (ajouter 156 patrouilles dans JORASYS), mais que cette opération a été déléguée par la BAC à Xplain, après que l'employé de la Police militaire a indiqué que l'opération lui prenait beaucoup de temps.

431 Il est ainsi superflu d'examiner si l'autorité responsable avait donné son accord écrit à l'accès par Xplain ou si des mesures avaient été mises en place pour éviter l'accès par des tiers aux données remises à Xplain.

432 En résumé, à notre sens, l'envoi par e-mail du fichier en cause à Xplain n'apparaît pas conforme à l'aOIAF en vigueur au moment des faits.

(iii) *Classification des informations*

433 D'après la classification adoptée par le DDPS, les informations contenues dans JORASYS relèvent de l'échelon « CONFIDENTIEL » au sens de l'art. 6 aOPrl dans sa teneur en juillet 2020[288].

434 Selon l'art. 13 al. 1 et 2 aOPrl dans sa teneur en juillet 2020, « *[l]'établissement d'informations classifiées, leur communication et le fait de les rendre accessibles doivent être limités à un strict minimum; à cet égard, la situation, la mission, l'objectif et le temps doivent être pris en considération. Il n'est permis de communiquer ou de rendre accessibles des informations classifiées qu'aux personnes qui doivent en avoir connaissance*. »

435 Comme exposé plus haut, il n'existait à notre sens aucune nécessité de communiquer les informations contenues dans le fichier Excel en question à Xplain, soit un fournisseur externe, dans le contexte en question.

436 Par conséquent, l'envoi par e-mail du fichier à un employé de Xplain n'apparaît pas conforme à l'aOPrl en vigueur au moment des faits.

437 Le fait que le fichier Excel ne contienne pas la mention "CONFIDENTIEL" apparaît en outre incompatible avec les prescriptions de l'aOPrl.

(iv) *Protection des données*

438 Dans la mesure où la LSIA ne contenait pas de dispositions spécifiques, la aLPD s'appliquait, et la LPD s'applique actuellement, au système JORASYS de la Police militaire (art. 1 al. 3 LSIA).

439 Le fichier Excel « [redacted] *.xls* » contient à l'évidence des données personnelles. La Police militaire doit être qualifiée de « maître du fichier » au sens de la aLPD (c'est-à-dire « responsable du traitement » selon la terminologie de la LPD).

440 Comme exposé plus haut, il n'existait à notre sens aucune nécessité de communiquer les informations contenues dans le fichier Excel en question à Xplain, soit un fournisseur externe, dans le contexte en question.

[288] Cf. [redacted] pdf (AUD 03.10.09.223).

441 Xplain procède *de facto* à un traitement de données personnelles sur instruction de la BAC. En effet, Xplain reçoit un fichier Excel contenant des données personnelles et établit un script en format .sql dans lequel Xplain intègrent ces mêmes données personnelles (« [redacted] .sql »[289].

442 Or, il résulte de l'enquête que les contrats relatifs à JORASYS ne prévoyaient pas, et *a fortiori* n'encadraient pas, la sous-traitance par Xplain. L'exigence centrale posée par l'art. 10a aLPD n'apparait ainsi pas respectée[290].

443 L'art. 2*a*[bis] l'OSIAr réglant également la sous-traitance n'est entré en vigueur que le 1[er] avril 2023[291], soit après les faits discutés ici.

444 En n'encadrant pas contractuellement ce rapport de sous-traitance, la BAC n'a, *a fortiori,* pas eu de visibilité sur la localisation des traitements et le recours éventuel à des sous-sous-traitants (étant rappelé que Xplain dispose de bureaux à l'étranger exploités par des filiales sises en Espagne et en Allemagne)[292].

445 En définitive, le cas d'espèce consacre *prima facie* des traitements non autorisés au sens de l'art. 7 aLPD, qui violent l'art. 12 al. 2 let. a aLPD, dans sa teneur en septembre 2010. Aucun des motifs justificatifs de l'art. 13 aLPD ne nous paraît donné en l'espèce[293].

446 Quant à l'art. 7 OTUIC, dont la teneur n'a pas évolué depuis son entrée en vigueur en 2012, et pour autant qu'il soit applicable (il est intitulé : « Traitement lié à des travaux techniques »), il n'autorise un traitement lié à des travaux techniques que si l'accomplissement de ces travaux *l'exige* (art. 7 al. 1 OTUIC). Or, nous avons vu que l'envoi à Xplain de ce fichier Excel n'était pas nécessaire en l'espèce. Cette disposition est donc potentiellement également violée.

(v) *Déficiences en matière technique, d'organisation ou de processus*

447 Il s'agit désormais d'examiner les ordonnances administratives pertinentes en l'espèce et l'existence d'éventuelles déficiences en matière technique, d'organisation ou de processus.

448 Parmi les textes qui lui ont été remis, OA a identifié le « *Handbuch IT-Sicherheit VBS* »[294], du 12 juillet 2011 (version 3.2). Ce document de 104 pages contient de nombreuses règles notamment sur l'organisation de la sécurité IT. En particulier, on y trouve une section 6.2.2 relative aux exigences de sécurité des entreprises tierces (« *Sicherheits-Anforderungen in Aufträgen mit Fremd-Unternehmen (BSE)* »). La section 10.7.3.1 dispose que le classement doit être sûr (« *Sämtliche Daten müssen entsprechend ihrem Schutzbedarf "sicher" abgelegt* »). En outre, la section 10.7.4.1. limite l'accès aux documents du sytème (« *System-Dokumentationen dürfen nur Berechtigten zugänglich sein*. »).

449 Afin d'éviter des répétitions, il peut être renvoyé *mutatis mutandis* à l'analyse des déficiences en matière technique, d'organisation ou de processus qui a été faite dans le premier cas ci-dessus.

---

[289] AUD B03.10.05.03.
[290] Sur la question des trois *curae*, cf. ci-dessous par. 499 ss.
[291] RO 2023 133.
[292] Cf. *supra* par. 214-217.
[293] Lorsqu'elle sollicite l'assistance ce fournisseur externe, la BAC « agit selon le droit privé » au sens de l'art. 23 aLPD (art. 40 LPD). La BAC était donc soumise aux dispositions de la aLPD applicables aux personnes privées et non à celles applicables aux organes fédéraux. Dans cette mesure, l'exigence de la base légale ne s'applique pas ici (art. 17 al. 1 aLPD applicable aux organes fédéraux).
[294] AUD B03.05.39.

g) Cas de transfert actif n° 3 : la capture d'écran d'un extrait d'une audition (12 janvier 2018)

450 L'analyse ci-dessus (let. a) s'applique pour l'essentiel au présent cas. En substance, celui-ci concerne l'envoi, le 12 janvier 2018, par un employé de fedpol (F) depuis son adresse [F]@fedpol.admin.ch d'un e-mail non chiffré intitulé « *WG :* [redacted] *(* » à un employé de Xplain (T), à son adresse [T]@xplain.ch.

451 Dans cet e-mail, F informe T au sujet de problèmes d'affichage des documents générés dans ORMA et sollicite son assistance[295]. Son e-mail comprend une capture d'écran d'un procès-verbal d'une audition apparemment menée par fedpol. Le nom et le prénom de la personne entendue sont visibles de même que ses déclarations (non verbatim).

452 En résumé, les normes spéciales applicables à ORMA (notamment la LSIP) ainsi que les dispositions en matière de sécurité de l'information (aOIAF) et en matière de classification des informations (aOPrI) apparaissent *prima facie* ne pas avoir été respectées. Le même constat s'applique aux dispositions en matière de protection des données (aLPD).

453 L'examen des déficiences en matière technique, d'organisation ou de processus contribuant à expliquer l'envoi à l'employé de Xplain des documents en cause, en violation des normes examinées dans les sections précédentes, a déjà été exposé ci-dessus, de sorte qu'il convient d'y renvoyer.

h) Cas de transfert actif n° 4 : une vidéo transmise dans le cadre d'une demande de support, révélant des noms/adresses de prévenus, témoins, avocats et enquêteurs d'une procédure pénale (12 décembre 2014)

454 L'analyse exposée ci-dessus (let. a) s'applique pour l'essentiel au présent cas. En substance, celui-ci concerne l'envoi, le 12 décembre 2014, par un employé de fedpol (F) depuis son adresse [F]@fedpol.admin d'un e-mail non chiffré intitulé « *Fwd:* [redacted] .» à S, à son adresse [S]@xplain.ch.

455 L'e-mail contient une pièce jointe intitulée « [redacted] *zip* ». Ce fichier compressé (.zip) contient à son tour un fichier « [redacted] *.MP4* »[296]. En substance, il s'agit d'un enregistrement vidéo de 71 secondes, lequel reproduit une assistance informatique à distance (« *Windows Remoteunterstützung* ») fournie à un enquêteur fedpol. Le procès-verbal d'une audition de témoin déléguée à fedpol par le Ministère public de la Confédération dans le cadre d'une procédure pénale est visible à l'écran.

456 En résumé, les normes spéciales applicables à ORMA (notamment la LSIP) ainsi que les dispositions en matière de sécurité de l'information (aOIAF) et en matière de classification des informations (aOPrI) apparaissent *prima facie* ne pas avoir été respectées. Le même constat s'applique aux dispositions en matière de protection des données (aLPD).

457 L'examen des déficiences en matière technique, d'organisation ou de processus contribuant à expliquer l'envoi à l'employé de Xplain des documents en cause, en violation des normes examinées dans les sections précédentes, a déjà été exposé ci-dessus, de sorte qu'il convient d'y renvoyer.

i) Cas de transfert « semi-automatique » : la fonctionnalité Error Reporting

458 L'analyse exposée ci-dessus s'applique pour l'essentiel à la fonction dite « *Error Reporting* ».

[295] AUD 03.10.02.26-31.
[296] AUD B03.10.02.09.

459 Le cas choisi ci-dessus pour illustrer cette fonction date du 24 octobre 2016. A cette date, M, un employé de l'OFDF, met à disposition de Y, un employé de Xplain dont la signature automatique au pied d'un e-mail suggère qu'il travaille en Allemagne, un fichier .zip sur le serveur T:\EFD\EZV\GWK ZEMIS de la Confédération.

460 Ce fichier compressé représente environ 21 Mo. Il contient des captures d'écran de pièces d'identités de personnes. En substance, le nom, le prénom, la nationalité et, dans un cas la photo d'identité, des personnes en question sont visibles

461 En résumé, les normes spéciales applicables à SYMIC (« *ZEMIS* ») (ordonnance sur le système d'information central sur la migration [Ordonnance SYMIC][297]), ainsi que les dispositions en matière de sécurité de l'information (aOIAF) et en matière de classification des informations (aOPrI) apparaissent *prima facie* ne pas avoir été respectées. Le même constat s'applique aux dispositions en matière de protection des données (aLPD).

462 L'examen des déficiences en matière technique, d'organisation ou de processus contribuant à expliquer l'envoi à l'employé de Xplain des documents en cause, en violation des normes examinées dans les sections précédentes, a déjà été exposé ci-dessus, de sorte qu'il convient d'y renvoyer.

B. Est-ce que la Confédération a rempli ses devoirs en matière de choix, d'instruction, de surveillance et de collaboration avec Xplain AG ?

463 La question posée part de la prémisse que la Confédération a des devoirs en matière de choix, d'instruction et de surveillance d'un prestataire de service externe ou un fournisseur ainsi que dans la collaboration avec ce dernier.

464 Il s'agit donc dans un premier temps (ch. 1) d'examiner la validité de cette prémisse, avant de nous prononcer dans le cas d'espèce (ch. 2).

1. Règles de droit pertinentes

465 La présente section a pour but de passer en revue les sources du droit pouvant fonder des obligations de l'administration fédérale en matière de choix, d'instruction, de surveillance et dans le domaine de la collaboration avec un prestataire de service externe ou un fournisseur. Nous examinons les règles de droit administratif général (*a*) avant d'en venir aux règles spéciales (*b*).

a) Droit administratif général

(i) *Introduction*

466 La complexité, l'éclatement et la diversité des formes qui caractérisent aujourd'hui l'organisation de l'administration en Suisse rendent particulièrement difficile la classification des entités administratives. Une partie de la doctrine adopte une classification tripartite (administration centrale, administration décentralisée [composée uniquement d'entités de droit public] et personnes privées chargées de tâches publiques). Une autre partie privilégie une classification bipartite (administration centralisée et administration décentralisée, regroupant toutes les entités – quelles que soient leur forme et leur nature juridique – n'appartenant pas à l'administration centralisée et chargées de tâches publiques[298]).

[297] RS 142.513.

[298] THIERRY TANQUEREL, Manuel de droit administratif, 2e éd., 2018, N 114 et N 115a et les références.

467 Des questions de délimitation se posent notamment lorsque les collectivités attribuent des tâches à des personnes extérieures à l'administration[299]. Dans ce contexte, on distingue notamment les concepts de *délégation de tâches publiques* et d'*activités administratives auxiliaires*.

(ii) *Délégation de tâches publiques et activités administratives auxiliaires*

468 Selon la Constitution fédérale, la loi peut confier des tâches de l'administration à des organismes et à des personnes de droit public ou de droit privé qui sont extérieurs à l'administration fédérale (art. 178 al. 3Cst.). Un délégataire est ainsi la personne qui exécute une *tâche publique* sur la base d'une délégation de compétence[300].

469 En revanche, relève des *activités administratives auxiliaires* (ou administration auxiliaire ; « *Hilfstätigkeit* », « *Bedarfsverwaltung* ») la fourniture de biens ou de prestations dont la production ne constitue pas en elle-même une tâche publique[301] (à savoir une tâche de l'administration), mais qui sont nécessaires à l'accomplissement de telles tâches. Au lieu de se procurer ces biens ou ces prestations par ses propres services, l'administration peut recourir à des tiers. On parlera fréquemment d' « *outsourcing* », parfois de sous-traitance[302].

470 La distinction entre *tâche publique* et *activité administrative auxiliaire* a notamment pour conséquence que les conditions de la délégation s'appliquent dans le premier cas (exigence d'une base légale [art. 178 al. 3 Cst.][303] voire constitutionnelle, intérêt public, respect du principe de spécialité et aménagement de pouvoirs de surveillance [obligation de respecter les droits fondamentaux selon l'art. 35 al. 2 Cst. ; art. 187 al. 1 a Cst.])[304] et non dans le second.

471 Les activités de support administratif comme l'acquisition de biens et de services (p. ex. entretien de bureaux, constructions d'ouvrages ou services financiers) relèvent du droit privé, selon la doctrine[305].

472 La doctrine fournit d'autres exemples d'activités administratives auxiliaires : la livraison de tramways, d'autobus, d'ordinateurs, d'appareils médicaux, de matériel de bureau entre dans la catégorie des activités administratives auxiliaires, tout comme la fourniture de services informatiques ou juridiques ou des travaux de construction ou d'entretien (y compris le nettoyage) effectués sur des infrastructures ou des bâtiments publics. Ainsi, la production d'ordinateurs ou la construction de bâtiments ne sont pas des tâches publiques, mais des activités économiques exercées par le secteur privé et dont l'administration a

---

[299] THIERRY TANQUEREL, Manuel de droit administratif, 2e éd., 2018, N 115.
[300] MICHAEL MONTAVON, Cyberadministration et protection des données, Fribourg 2021, p. 768 s.
[301] Le concept de tâches publiques n'est guère unifié. On peut néanmoins relever que, selon le Tribunal fédéral, les tâches publiques sont déterminées par la Constitution et les lois et procèdent d'un choix politique (ATF 138 II 134 consid. 4.3.1 ; cf. également BLAISE KNAPP, L'exécution des tâches publiques fédérales par des tiers, in SBVR vol. I, 1996, nos 3 ss). Des auteurs de doctrine proposent pour leur part une définition plus extensive : sont des *tâches publiques*, pour lesquelles la question de l'externalisation est *a priori* susceptible de se poser, d'abord les tâches qui, par définition, ne peuvent incomber originairement qu'à l'Etat : ce sont toutes les tâches qui impliquent l'exercice de la puissance publique. S'y ajoutent toutes les tâches matérielles qui sont de la responsabilité de l'Etat, en vertu de la Constitution, de la loi ou d'un choix d'une collectivité publique, voire d'une entité décentralisée, opéré dans les limites d'un pouvoir d'appréciation conféré par la loi. Y sont également assimilées les activités exercées par l'Etat ou concédées par lui dans le cadre d'un monopole, dans la mesure où leur externalisation ne leur ferait pas perdre leur caractère d'intérêt public (PIERRE MOOR/FRANÇOIS BELLANGER/THIERRY TANQUEREL, Droit administratif, vol. III, 2e éd., 2018, p. 140).
[302] PIERRE MOOR/ François BELLANGER/THIERRY TANQUEREL, Droit administratif, vol. III, 2e éd., 2018, p. 141 et p. 244 s.
[303] MICHAEL MONTAVON, Cyberadministration et protection des données, Fribourg 2021, p. 252.
[304] PIERRE MOOR/ FRANÇOIS BELLANGER/THIERRY TANQUEREL, Droit administratif, vol. III, 2e éd., 2018, p. 208, p. 210 et p. 245 s.
[305] TEO GENECAND, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 4 ad art. 40 LPD.

pour exécuter ses tâches. L'expert informatique est un prestataire privé auxiliaire, chargé de corriger une erreur logicielle dans un programme utilisé par l'administration. Il s'agit ici d'activités administratives auxiliaires, que l'administration aurait tout aussi bien pu accomplir par son propre personnel, mais qu'elle a choisi de se procurer sur le marché jugeant que celui-ci les offrait à satisfaction[306]. Un autre auteur retient également que les services informatiques constituent *a priori* des activités administratives auxiliaires (« *Bedarfsverwaltung* »)[307].

473 Il a toutefois récemment été soutenu par un auteur que la sophistication toujours plus avancée de ces services, le rôle toujours plus important et stratégique qu'ils occupent dorénavant dans le fonctionnement et l'organisation de l'État et les nouveaux risques qu'ils amènent viennent aujourd'hui remettre cette qualification en question, en partie en tout cas. Selon cet auteur, dans certains cas, la fourniture de services informatiques dépasse les contours d'une tâche auxiliaire et peut correspondre à la délégation d'une véritable tâche publique, impliquant le respect des conditions précitées (exigence de la base légale ([art. 178 al. 3 Cst.] et obligation des fournisseurs de respecter eux-mêmes les droits fondamentaux des personnes concernées [cf. art. 35 al. 2 Cst.])[308].

(iii) *Activités administratives auxiliaires régies en principe par le droit privé*

474 En principe, la sous-traitance par un organe fédéral peut reposer sur un contrat ; s'il s'agit d'activités administratives auxiliaires, les règles des marchés publics trouveront application à la naissance de la relation contractuelle, la relation entre la collectivité et l'entreprise privée délivrant les prestations étant pour sa part régie par le droit privé[309].

475 La loi impose néanmoins certaines obligations à charge du sous-traitant, que le contrat reprend et précise généralement. En matière de protection des données personnelles, le sous-traitant est ainsi tenu de prendre les mesures organisationnelles et techniques appropriées selon l'art. 8 LPD. En outre, il ne saurait s'écarter du cadre légal établi et procéder à des traitements de données que l'organe public ne serait pas en droit d'accomplir lui-même (cf. art. 9 al. 1 let. a LPD)[310].

476 Dans le domaine informatique, la qualification du contrat s'effectue à l'aune des circonstances du cas d'espèce. Les contrats portant sur des services informatiques constituent fréquemment des contrats innommés ou mixtes. Ils peuvent selon les circonstances se rapprocher du contrat de mandat, d'entreprise, de licence, voire de vente ou de bail[311].

b) *Règles spéciales pertinentes*

477 Notre analyse ci-dessous (ch. 2) tiendra compte des règles qui étaient en vigueur au moment des faits et qui se trouvaient dans l'aLPD, l'aOPrl, l'aOIAF, l'aOPCy et l'OTNI (voir le tableau général *supra* par. 256).

[306] Pierre Moor/ François Bellanger/Thierry Tanquerel, Droit administratif, vol. III, 2e éd., 2018, p. 141 et p. 245 s.
[307] Rolf H. Weber, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl 100/1999, p. 97, 102 et 107.
[308] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, p. 768 s.
[309] Pierre Moor/ François Bellanger/Thierry Tanquerel, Droit administratif, vol. III, 2e éd., 2018, p. 141 s. et 245.
[310] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, p. 250.
[311] Emilie Jacot-Guillarmod, in Benhamou/Cottier (éd.), Petit commentaire LPD, 2023, N 9 ad art. 9 LPD.

(i) *Devoir de choisir avec soin*

478 Le devoir de choisir avec soin le sous-traitant (« *Auftragsbearbeiter* » ou « *Processor* ») qui traite des données personnelles, qui découlait des art. 14 puis 10a aLPD, a été examinée plus haut, de sorte qu'on y renvoie[312].

479 Selon l'art. 8 aOIAF (en vigueur entre 2003 et 2012), puis l'art. 10 aOIAF (en vigueur de 2012 à 2021), puis l'art. 14 al. 2 aOPCy (en vigueur en 2020) et enfin l'art. 14 al. 3 let. a aOPCy (en vigueur de 2021 à 2023), les unités administratives sont responsables de la sécurité de leurs objets informatiques à protéger[313], elles font l'inventaire de leurs objets informatiques à protéger et prennent les mesures de sécurité nécessaires.

480 Selon l'art. 24 al. 3 aOIAF (« Acquisition de prestations en TIC auprès de fournisseurs de prestations »), en vigueur de 2003 à 2012, les adjudicateurs choisissent la solution présentant le meilleur rapport coûts-utilité et présentant le moins de risques.

481 Selon l'art. 26a aOIAF (en vigueur de 2016 à 2021) et l'art. 11 OTNI (en vigueur depuis 2021), les fournisseurs externes de prestations informatiques peuvent obtenir l'accès à des données qui ne sont pas accessibles au public si les conditions suivantes sont réunies: (a) cet accès est nécessaire pour la fourniture des prestations informatiques; (b) l'autorité responsable des données a donné son accord écrit; (c) il a été pris les mesures contractuelles, organisationnelles et techniques garantissant que les données ne seront pas accessibles à des tiers. Il en découle à notre sens un devoir de choisir avec soin le fournisseur en question.

(ii) *Devoir d'instruire adéquatement*

482 Le devoir d'instruire adéquatement le sous-traitant qui traite des données personnelles, qui découlait des art. 14 puis 10a aLPD, a été examinée plus haut, de sorte qu'on y renvoie[314].

483 Les art. 8 aOIAF (2003 à 2012), 10 aOIAF (2012 à 2021), 26a aOIAF (2016-2021) et 11 OTNI (dès 2021), dont on peut, à notre sens, déduire un devoir d'instruire avec soin un prestataire externe de prestations informatiques, ont été exposés ci-dessus de sorte qu'on y renvoie également[315].

484 Selon l'art. 25 al. 2 aOIAF (en vigueur de 2012 à 2021), en cas d'acquisitions de prestations auprès d'un fournisseur externe, les directives concernant les TIC font partie intégrante du dossier d'appel d'offres.

485 Une règle analogue résulte de l'art. 14 al. 2 let. d aOPCy (en vigueur en 2020), respectivement de l'art. 14 al. 3 let. d aOPCy (en vigueur de 2021 à 2023), selon laquelle les unités administratives doivent s'assurer qu'en cas d'acquisition de prestations auprès d'un fournisseur externe les directives en matière de sécurité informatique font partie intégrante du contrat.

(iii) *Devoir de surveiller*

486 Le devoir de surveiller le sous-traitant qui traite des données personnelles, qui découlait des art. 14 puis 10a aLPD, a été examinée plus haut, de sorte qu'on y renvoie[316].

---

[312] Cf. par. 292-300.
[313] La formulation a évolué au gré des révisions des ordonnances et nous citons ici l'art. 14 al. 3 let. a aOPCY entré en vigueur le 1er avril 2021.
[314] Cf. par. 292-300.
[315] Cf. par. 308.
[316] Cf. par. 292-300.

487 L'art. 13 aOIAF (en vigueur de 2000 à 2003), puis l'art. 26 aOIAF (en vigueur de 2003 à 2012), donnaient au Contrôle fédéral des finances la compétence d'effectuer des audits de l'informatique.

488 Selon l'art. 25 al. 3 aOIAF (en vigueur de 2012 à 2021), en cas d'acquisitions de prestations auprès d'un fournisseur externe, le bénéficiaire des prestations vérifie de façon appropriée le respect des directives concernant les TIC par le fournisseur externe.

489 Une règle analogue résulte de l'art. 14 al. 2 let. e aOPCy (en vigueur en 2020), respectivement de l'art. 14 al. 3 let. e aOPCy (en vigueur de 2021 à 2023), selon laquelle les unités administratives doivent vérifier de manière appropriée que les directives en matière de sécurité informatique sont respectées par les fournisseurs externes.

2. En l'espèce

a) Absence de devoirs généraux de choisir, instruire et surveiller avec soin

490 La présente enquête porte sur les relations de la Confédération avec un acteur privé, Xplain. Il convient donc de discuter brièvement la question de la décentralisation de l'activité administrative et des conditions qui pourraient en résulter, notamment en termes d'obligation de surveillance.

491 Il a été soutenu que le domaine de la cybersécurité devrait être considéré comme un domaine de la sécurité à proprement parler, non susceptible de délégation à une entité privée[317] ou seulement à des conditions très strictes : l'Etat assumerait son obligation de garant (notamment : contrôle de l'exécution des tâches, contrôle par l'Etat du respect des droits fondamentaux) et la responsabilité finale de la sécurité publique[318]. Suivant cette hypothèse, les services fournis par Xplain seraient alors soumis à des obligations de contrôles strictes, ce qui influencerait les conclusions de la présente enquête.

492 Cela étant, *de lega lata*, nous retenons que les tâches convenues contractuellement avec Xplain – en particulier la création, le développement ou la maintenance de logiciels, ainsi que le support informatique – ne constituent en principe pas des tâches publiques, mais des activités administratives auxiliaires. Les services fournis par Xplain ainsi que les produits livrés (*software*) doivent être qualifiés *d'activités administratives auxiliaires*, dans le même sens que les exemples fournis par la doctrine ci-dessus[319]. En effet, ces services et produits ne constituent pas en eux-mêmes une tâche publique dont la délégation – qui serait d'ailleurs nécessairement soumise à base légale – devrait faire automatiquement l'objet d'une surveillance en vertu du droit administratif général de la décentralisation de l'activité administrative.

493 Par conséquent, ce sont les règles spéciales qui ont été citée plus haut qui fondaient les devoirs des Unités directement concernées en matière de choix, d'instruction et de surveillance de Xplain.

---

[317] Selon des auteurs, la privatisation des tâches entières du domaine de la sécurité publique n'est pas admissible d'un point de vue constitutionnel (MICHAEL GUERY, La privatisation de la sécurité et ses limites juridiques, SJ 2006 II p. 141, 158 s. ; ETIENNE POLTIER, CR Cst., Art. 81-Disp. fin., 2021, N 48 ad art. 178 Cst. ; voir aussi ROLF H. WEBER, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl 100/1999, p. 97, 100, qui considère toutefois la privatisation exclue dans seulement quelques cas exceptionnels [par exemple usage de la force]).

[318] MICHAEL GUERY, La privatisation de la sécurité et ses limites juridiques, SJ 2006 II p. 141, 158 s.

[319] Par. 471-472.

b) Application des règles spéciales

(i) *Est-ce que le devoir de choisir avec soin a été rempli ?*

494 Sous l'angle de la sécurité de l'information, le Conseil de l'informatique de la Confédération a émis des directives le 27 septembre 2004 afin de concrétiser les exigences de l'aOIAF. Celles-ci ont été remplacées par des directives du Conseil fédéral du 14 août 2013 puis du 1er juillet 2015 concernant la sécurité des TIC dans l'administration fédérale et enfin par les directives du Conseil fédéral du 16 janvier 2019 concernant la sécurité informatique dans l'administration fédérale.

495 Ces directives prévoient toutes, en substance et entre autres règles, que tout projet informatique doit faire l'objet d'une analyse des besoins de protection (« *Schutzbedarfanalyse* »). Si l'analyse révèle des besoins de protection élevés, un concept SIPD (« concept de sécurité de l'information et de protection des données ») doit être élaboré.

496 Sur la base des documents revus et des interrogatoires qui ont été menés dans la présente enquête administrative, il apparaît que ces exigences ont été respectées par les Unités directement concernées dans chaque projet informatique avec Xplain.

497 Sous l'angle de l'art. 24 al. 3 aOIAF (2003 à 2012), ainsi que sous l'angle des art. 26a aOIAF (2016 à 2021) et 11 OTNI (dès 2021), on peut néanmoins relever qu'il est établi que les Unités directement concernées n'ont jamais sollicité, ni *a fortiori* obtenu, de rapport sur la sécurité de l'information au sein de Xplain avant de débuter ou renouveler des relations contractuelles. Ce n'est qu'après la fuite de données de juin 2023 que Xplain a fait l'objet d'un audit mandaté par la Confédération, dont l'existence a été mentionnée par plusieurs personnes interrogées.

498 Ainsi, l'Organe d'enquête parvient à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération a partiellement rempli son devoir de choisir avec soin, sous l'angle des normes précitées de la sécurité de l'information.

499 Sous l'angle de la protection des données personnelles, nous avons examiné plus haut certains cas (n° 4 « extraction ORMA »[320] et n° 6 « patrouilles JORASYS »[321]) dans lesquels Xplain doit à notre sens être qualifié de sous-traitant au sens de la aLPD et de la LPD. Nous avons vu également que ces cas de sous-traitance ne faisaient, à notre connaissance, pas l'objet d'un contrat, contrairement à l'exigence posée par les art. 14 puis 10a aLPD applicables à l'époque des faits[322]. Il faut donc *a fortiori* constater que la Confédération n'a pas choisi avec soin le sous-traitant auquel un traitement de données personnelles a été confié dans les cas en question.

500 Ainsi, sous l'angle de la protection des données personnelles, l'Organe d'enquête parvient à la conclusion que la Confédération n'a pas rempli son devoir de choisir avec soin dans les cas de sous-traitance qui ont été identifiés.

(ii) *Est-ce que le devoir d'instruire adéquatement a été rempli ?*

501 Sous l'angle de la sécurité de l'information, les contrats remis à OA contiennent tous des renvois à des conditions générales de la Confédération (« **CG** ») en matière informatique, qu'il s'agisse des CG pour l'achat de matériel informatique, des CG pour l'acquisition et la maintenance de logiciels standards, des

[320] Cf. *supra* section IV.A.4.
[321] Cf. *supra* section IV.A.6.
[322] Actuellement : art. 9 LPD.

CG pour les contrats d'entreprise dans le domaine informatique et pour la maintenance de logiciels individuels, des CG pour les services informatiques ou de précédentes éditions de ces CG.

502 Les CG éditées en octobre 2010 et en janvier 2021 incluent une obligation de « maintien du secret » (*« Geheimhaltung »*). Celle-ci prévoit notamment que

> *Les parties traitent de manière confidentielle tous les faits et informations qui ne sont pas publics ni accessibles au public. En cas de doute, elles traiteront les faits et informations de manière confidentielle. Les parties s'engagent à prendre toutes les mesures que l'on peut raisonnablement attendre d'elles du point de vue économique et toutes les mesures techniques et organisationnelles possibles, de manière que des faits et informations confidentiels soient interdits d'accès et ne parviennent pas à la connaissance de tiers non autorisés. (…)*
>
> *Les parties imposent l'obligation de garder le secret à leurs collaborateurs, à leurs sous-traitants, à leurs fournisseurs et aux autres tiers auxquels elles font appel.*

503 Cette clause n'existait pas dans les CG applicables de juin 1998 jusqu'en octobre 2010.

504 Les CG éditées en octobre 2010 et en janvier 2021 contiennent une clause générale de protection et sécurité des données :

> *Les parties s'engagent à respecter les dispositions de la législation suisse sur la protection des données. Elles s'engagent à prendre toutes les mesures que l'on peut raisonnablement attendre d'elles du point de vue économique et toutes les mesures techniques et organisationnelles possibles, de manière que les données produites et échangées dans le cadre de l'exécution du contrat ne parviennent pas à la connaissance de tiers non autorisés.*
>
> *Les données personnelles ne peuvent être traitées que dans la mesure où cela est nécessaire à l'exécution du contrat. En outre, elles peuvent être transmises à une entreprise liée à l'une des parties au contrat et établie en Suisse ou à l'étranger, à condition que cela soit nécessaire à l'exécution du contrat et que les dispositions de la législation suisse sur la protection des données soient respectées.*
>
> *Les parties imposent ces obligations à leurs collaborateurs, à leurs sous-traitants, à leurs fournisseurs et aux autres tiers prêtant leur concours à l'exécution du contrat.*

505 Cette clause n'existait pas dans les CG applicables de juin 1998 jusqu'en octobre 2010.

506 Les CG de la Confédération en matière informatique ne contiennent au surplus aucune clause sur les obligations du prestataire externe en matière de cybersécurité ou de sécurité de l'information.

507 L'obligation d'intégrer les directives concernant les TIC (renommées directives en matière de sécurité informatique) au dossier d'appel d'offres (selon l'art. 25 al. 2 aOIAF), respectivement au contrat (selon l'art. 14 al. 2 let. d puis l'art. 14 al. 3 let. d aOPCy) a été partiellement respectée au vu des contrats qui nous ont été remis par les Unités concernées.

508 De nombreux contrats contiennent ces directives en annexes ou y renvoient. Dans un cas isolé, un *Bearbeitungsreglement* annexé au contrat y renvoie[323]. L'enquête a toutefois révélé que des contrats n'intégraient pas ces directives. Cette dernière situation concerne particulièrement fedpol, qui ne paraît

[323] Vertrag Nr [redacted] für die Erbringung von werkvertraglichen Leistungen im Informatikbereich und die Pflege von Individualsoftware (Werkvertrag) (AUD B03.04.10.174).

pas avoir intégré ces directives dans les contrats qui nous ont été remis, à l'exception du contrat précité qui y renvoie *via* le *Bearbeitungsreglement*[324].

509 Aucun des contrats conclus avant juillet 2020 et qui nous ont été remis ne contiennent de clauses spécifiques sur la sécurité de l'information.

510 A compter de la publication le 1er septembre 2020 par la Conférence des achats de la Confédération (« CA ») de la Clause contractuelle type de la CA pour les cyberrisques, cette clause a été intégrée dans plusieurs contrats et avenants conclus avec Xplain qui nous ont été remis par les Unités touchées par l'enquête, mais pas dans tous :

	Contrats et avenants[325] postérieurs au 1er septembre 2020	*Dont : intégrant la Clause contractuelle type pour les cyberrisques*
DFAE	0	*0*
armasuisse	0	*0*
BAC	0	*0*
PM	N/A	*N/A*
SRC	0	*0*
OFDF	3	*0*
OFCL	0	*0*
OFIT	0	*0*
fedpol	7	*6*
OFJ	14	*2*
SEM	0	*0*
CSI-DFJP	0	*0*

511 Ainsi, l'Organe d'enquête parvient à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération a partiellement rempli son devoir d'instruire adéquatement, sous l'angle des normes précitées de la sécurité de l'information.

512 Sous l'angle de la protection des données personnelles, nous avons examiné plus haut certains cas (n° 3 « extraction ORMA »[326] et n° 5 « patrouilles JORASYS »[327]) dans lesquels Xplain doit à notre sens être qualifié de sous-traitant au sens de la aLPD et de la LPD. Nous avons vu également que ces cas de sous-traitance ne faisaient, à notre connaissance, pas l'objet d'un contrat contrairement à l'exigence posée par les art. 14 puis 10a aLPD applicables à l'époque des faits[328]. Il faut donc *a fortiori* constater que la Confédération n'a pas instruit adéquatement le sous-traitant auquel un traitement de données personnelles a été confié dans les cas en question.

513 Ainsi, sous l'angle de la protection des données personnelles, l'Organe d'enquête parvient à la conclusion que la Confédération n'a pas rempli son devoir d'instruire adéquatement dans les cas de sous-traitance qui ont été identifiés.

[324] Vertrag [redacted] für die Erbringung von werkvertraglichen Leistungen im Informatikbereich und die Pflege von Individualsoftware (Werkvertrag) (AUD B03.04.10.174).
[325] Les commandes ne sont pas prises en compte.
[326] Cf. *supra* section IV.A.3.
[327] Cf. *supra* section IV.A.6.
[328] Actuellement : art. 9 LPD.

(iii) *Est-ce que le devoir de surveiller a été rempli ?*

514 Sous l'angle de la sécurité de l'information, il est établi que les Unités directement concernées n'ont jamais sollicité, ni *a fortiori* obtenu, de rapport sur la sécurité de l'information au sein de Xplain.

515 L'enquête n'a en outre identifié aucune déclaration « BSE » relative à Xplain[329].

516 De même, l'enquête n'a pas identifié de démarches des Unités directement concernées visant à vérifier de façon appropriée le respect des directives concernant les TIC par Xplain (art. 25 al. 3 aOIAF), respectivement à vérifier de manière appropriée que les directives en matière de sécurité informatique étaient respectées par Xplain (art. 14 al. 2 let. e aOPCy, puis art. 14 al. 3 let. e aOPCy).

517 Or, ces directives prévoyaient notamment que : « *[l]es fournisseurs de prestations mettent en œuvre les mesures de sécurité nécessaires lors de l'exploitation des moyens liés aux TIC[330], les documentent et les contrôlent. Ils transmettent les résultats aux bénéficiaires de prestations sous une forme appropriée* ».

518 L'enquête n'a pas non plus identifié de démarches des Unités directement concernées visant à vérifier que Xplain avait imposé l'obligation de garder le secret à ses filiales en Espagne et en Allemagne, en application des CG éditées en octobre 2010 et en janvier 2021. L'opinion exprimée dans plusieurs interrogatoires selon laquelle les relations entre Xplain et ses filiales à l'étranger ne concerneraient pas la Confédération ne peut pas être suivie.

519 Ainsi, l'Organe d'enquête parvient à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération n'a pas rempli son devoir de surveiller, sous l'angle des normes précitées de la sécurité de l'information.

520 Sous l'angle de la protection des données personnelles, nous avons examiné plus haut certains cas (n° 3 « extraction ORMA »[331] et n° 5 « patrouilles JORASYS »[332]) dans lesquels Xplain doit à notre sens être qualifié de sous-traitant au sens de la aLPD et de la LPD. Nous avons vu également que ces cas de sous-traitance ne faisaient, à notre connaissance, pas l'objet d'un contrat contrairement à l'exigence posée par les art. 14 puis 10a aLPD applicables à l'époque des faits[333]. Il faut donc *a fortiori* constater que la Confédération n'a pas surveillé le sous-traitant auquel un traitement de données personnelles a été confié dans les cas en question.

521 Ainsi, sous l'angle de la protection des données personnelles, l'Organe d'enquête parvient à la conclusion que la Confédération n'a pas rempli son devoir de surveiller dans les cas de sous-traitance qui ont été identifiés.

VI. PRINCIPAUX ENSEIGNEMENTS ET RECOMMANDATIONS

A. Principaux enseignements

1. Comment les données productives sont-elles parvenues chez Xplain ?

522 Au terme de l'enquête administrative, les circonstances factuelles qui ont conduit à ce que des données productives de certaines unités de la Confédération soient présentes dans l'environnement informatique de Xplain peuvent être résumées comme suit.

---

[329] Cf. *supra* par. 359.
[330] Les Directives du 16 janvier 2019 utilisent l'expression « moyens informatiques ».
[331] Cf. *supra* section IV.A.3.
[332] Cf. *supra* section IV.A.6.
[333] Actuellement: art. 9 LPD.

523 Premièrement, des employés de Xplain ont envoyé, depuis le compte e-mail de la Confédération mis à leur disposition dans le cadre de la collaboration entre Xplain et une Unité concernée, vers leur compte e-mail auprès de Xplain ou vers le compte e-mail de leurs collègues auprès de Xplain, des données productives reçues d'employés de la Confédération. Dans un cas à tout le moins, un employé de Xplain a selon toute vraisemblance extrait lui-même des données d'un système de production de fedpol et ces données se sont ensuite trouvées dans l'environnement informatique de Xplain.

524 Deuxièmement, des employés de la Confédération en charge du support informatique interne ont traité des demandes d'utilisateurs contenant des données productives et les ont transmises à Xplain ou les ont mises à disposition de Xplain sur un serveur partagé, sans préalablement retirer, pseudonymiser ou caviarder les données productives.

525 Troisièmement, des employés de la Confédération participant à des travaux de développement, de test ou de migration informatique, ont transmis à Xplain des données productives dans le cadre de ces travaux.

526 Nous ne pouvons pas définitivement exclure l'existence d'autres canaux ayant conduit à la présence de données productives de la Confédération dans l'environnement informatique de Xplain. S'agissant des données productives de la Confédération présentes sur le darknet suite à la fuite de données de juin 2023, la majorité semble être parvenue chez Xplain par les canaux de transmission identifiés dans le présent rapport. Pour une minorité de données, l'enquête n'a pas permis d'identifier le canal correspondant. En revanche, l'enquête a permis d'identifier des situations dans lesquelles des données productives de la Confédération sont parvenues dans l'environnement informatique de Xplain, sans que ces données ne se trouvent sur le darknet en juin 2023.

2. Quelle est l'ampleur des transmissions de données productives à Xplain ?

527 Les cas de transmission de données productives à Xplain apparaissent isolés, d'une part, à l'échelle de la correspondance entre Xplain et les Unités touchées par l'enquête et, d'autre part, à l'échelle de la correspondance entre Xplain et chaque employé de la Confédération ou chaque employé de Xplain ayant transmis à une occasion au moins des données productives à Xplain.

528 Toutefois, comme l'illustrent les cas examinés dans ce rapport, en matière de sécurité de l'information et de protection des données, un seul transfert à un tiers suffit potentiellement :

- Pour que la sécurité de l'information et la protection des données soient compromises.
- Pour que des volumes importants de données soient en mains d'un tiers.
- Pour que des données sensibles ou classifiées soient en mains d'un tiers.

3. Quelles étaient les déficiences en termes d'organisation, de processus ou de technique ?

529 Les principales déficiences mises en évidence par l'enquête administrative sont les suivantes.

530 Premièrement, une déficience en termes de processus : des employés de la Confédération et des employés d'un fournisseur externe, Xplain, ont pu extraire des données de systèmes de production de la Confédération et envoyer ces données par e-mail à Xplain sans qu'un processus n'encadre apparemment ces démarches et, en particulier, sans que le principe des quatre yeux ne soit respecté à chaque étape.

531 Deuxièmement, une déficience en termes de technique : aucune mesure technique n'est venue faire obstacle aux extractions de données productives précitées, ni à l'envoi par e-mail de données productives vers un fournisseur externe (p. ex. blocage automatique lorsqu'une extraction ou un envoi remplissent

des critères prédéfinis relatifs par exemple aux groupes d'utilisateurs, au volume, aux métadonnées ou au type de fichier).

532 Troisièmement, les cas décrits dans ce rapport mettent en lumière un déficit en termes de formation et de sensibilisation des personnes appelées à traiter des données des systèmes en question au sein de la Confédération. En outre, certaines Unités n'ont pas identifié que des applications développées par Xplain conduisaient potentiellement à des flux de données productives dans le cadre de demandes de support ; après qu'une unité a identifié cette fonctionnalité en 2020, l'information n'apparaît pas avoir circulé entre les Unités directement concernées.

4. Les devoirs en matière de choix, d'instruction et de surveillance ont-ils été respectés ?

533 Les tâches convenues contractuellement avec Xplain – en particulier la création, le développement ou la maintenance de logiciels, ainsi que le support informatique – ne constituent à notre sens pas des tâches publiques, mais des activités administratives auxiliaires. Sous l'angle du droit administratif général, l'Organe d'enquête retient donc que la Confédération n'avait pas à remplir les conditions d'une délégation de tâches publiques dans ses relations avec Xplain.

534 Sous l'angle de la sécurité de l'information, l'Organe d'enquête parvient à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération a partiellement rempli ses devoirs de choisir avec soin et d'instruire adéquatement. En revanche, le devoir de surveiller n'a pas été rempli dans ce contexte.

535 Sous l'angle de la protection des données personnelles, l'Organe d'enquête parvient à la conclusion que, dans les cas de sous-traitance à Xplain qui ont été identifiés, la Confédération n'a pas rempli ses devoirs de choisir avec soin, d'instruire adéquatement et de surveiller[334].

5. Dans quel contexte s'inscrivent les transmissions de données productives à Xplain et les manquements aux devoirs de choisir avec soin, instruire adéquatement et surveiller ?

536 Les cas de transmission de données productives à Xplain et les violations retenues par l'Organe d'enquête, du côté de la Confédération, aux devoirs de choisir avec soin, instruire adéquatement et surveiller sont intervenus dans un contexte factuel qu'il convient de résumer ici. Plusieurs facteurs nous paraissent en effet avoir favorisé – mais non causé – ces cas de transmissions de données et ces violations.

a) Lacunes en matière de gestion des cybermenaces des tiers

537 Le recours à des fournisseurs externes représente un enjeu sous l'angle de la sécurité de l'information à deux titres au moins.

538 D'une part, il s'agit de la sécurité de la chaîne d'approvisionnement (« *supply chain security* »)[335]. La notion se réfère à la sécurité des moyens informatiques[336] (en particulier des logiciels) développés par des tiers et acquis par une entreprise ou une collectivité publique[337]. La plupart des logiciels ne sont pas

[334] Cf. *supra* par. 494-521.
[335] Voir à titre illustratif aux Etats-Unis : Sec. 4 du Executive Order on Improving the Nation's Cybersecurity, 12 mai 2021.
[336] Art. 5 let. a LSI (en vigueur dès le 1er janvier 2014).
[337] Dans un sens plus large, la sécurité de la chaîne d'approvisionnement comprend également la sécurité des moyens informatiques qu'une entité de la Confédération développe ou acquiert et qu'elle met à disposition d'autres entités de la Confédération.

écrits à neuf et d'un seul tenant[338]. Lors de leur développement, des codes *open source* ou provenant de bibliothèques existantes y sont souvent intégrés[339]. Les vulnérabilités figurant dans ces éléments sont alors incorporées et diffusées de manière involontaire[340].

539 Lors d'une cyberattaque *via* la chaîne d'approvisionnement, l'attaquant vise d'abord un tiers afin de tenter d'atteindre ensuite, le cas échéant via un autre tiers, l'entreprise ou la collectivité publique[341]. En outre, « *[d]es attaques visant des logiciels ou du matériel pendant le processus de fabrication sont également imaginables. Le produit est alors livré avec un point faible, une porte dérobée ou un maliciel préinstallé* »[342]. Enfin, des dysfonctionnements ponctuels peuvent interrompre la chaîne (attaque *contre* la chaîne d'approvisionnement)[343].

540 Au terme de l'enquête, nous n'avons pas vu ou reçu des indications selon lesquelles ces risques se seraient réalisés dans le cas de Xplain[344]. En toute hypothèse, l'enquête administrative ne portait pas sur les circonstances dans lesquelles Xplain a fait l'objet de la fuite de données de juin 2023. L'enquête administrative était au contraire focalisée sur la Confédération.

541 D'autre part, le recours à des fournisseurs externes pose la question plus générale de la gestion des cybermenaces des tiers (« *third party cyber risk management* »). Cette question est centrale dans le cas présent. La gestion des cybermenaces des tiers désigne le processus systématique d'identification, d'analyse, d'évaluation et de gestion des cybermenaces que présentent les tiers avec lesquels une organisation partage certaines de ses données[345].

542 L'enquête a montré que la sécurité de l'information a été perçue par les Unités touchées par l'enquête, pour certaines jusqu'en 2019 ou 2020 environ et pour d'autres jusqu'à la fuite de données Xplain en 2023, comme une problématique essentiellement interne (les systèmes de la Confédération doivent être sécurisés/résilients face aux cybermenaces) et que les risques posés par les tiers ont généralement été sous-estimés, qu'il s'agisse du risque d'attaque via la chaîne d'approvisionnement ou des risques liés au partage de données avec un fournisseur externe. En particulier, les risques liés au recours à un fournisseur de logiciels, par opposition notamment à un fournisseur de services *cloud*, ont été sous-estimés.

b) Incertitudes sur les responsabilités en matière de sécurité de l'information

543 Les interrogatoires conduits par l'Organe d'enquête ont révélé des incertitudes, voire des positions contradictoires, concernant la répartition des responsabilités en matière de sécurité de l'information. Lors de la plupart des interrogatoires, la question a été posée de savoir qui (quelle unité, voire quelle personne au sein d'une unité) doit s'assurer de la sécurité de l'information en cas d'acquisition de

---

[338] NCSC, Sécurité de l'information, rapport semestriel 2021/II, p. 10.
[339] *Ibidem*.
[340] *Ibidem*.
[341] NCSC, Sécurité de l'information, rapport semestriel 2021/II, p. 7; cf. également FISSELER/SIEGMUND/MÖRSTEDT, Unterschätzte Risiken durch Lieferanten, digma 2018 p. 120, 122.
[342] NCSC, Sécurité de l'information, rapport semestriel 2021/II, p. 7.
[343] *Ibidem*.
[344] Voir à ce sujet les déclarations du Délégué fédéral à la cybersécurité de début juillet 2023 (rapportées notamment par Watson.ch, *Xplain-Hack war laut Bund kein gezielter Angriff auf den Bund*, 5 juillet 2023)
[345] Définition inspirée de plusieurs sources: Rapport du Conseil fédéral « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense », 24.11.2021, p. 8 ; JUDITH H. GERMANO, Third-Party Cyber Risk & Corporate Responsability, NYU Center for Cybersecurity, 2017 ; Ponemon Institute, Data Risk in the Third-Party Ecosystem: Third Annual Study, novembre 2018, p. 2.

prestations auprès d'un fournisseur externe (i) au cours du processus d'adjudication, (ii) lors de la négociation et la conclusion du contrat et (iii) au cours de la relation contractuelle.

544 La comparaison des réponses révèle des compréhensions parfois divergentes de la répartition des responsabilités entre, suivant les situations, (i) le service d'achat central au sens de l'art. 9 Org-OMP, (ii) l'unité administrative qui intervient comme service demandeur au sens de l'art. 3 let. b Org-OMP, (iii) le département auquel cette unité appartient, (iv) le CSI-DFJP, (v) l'OFIT, (vi) voire entre certains collaborateurs d'un même service.

545 Cette absence de compréhension uniforme des responsabilités entraîne un risque de conflits de compétence négatif.

c) Insuffisance des ressources allouées à la sécurité de l'information

546 Selon la vision exposée dans la Cyberstratégie nationale (CSN ; avril 2023), « *[l]a Suisse saisit les chances offertes par la transformation numérique et engage des mesures de protection pour réduire les cybermenaces et leurs conséquences. Elle compte parmi les leaders mondiaux en matière de connaissances, de formation et d'innovation dans le domaine de la cybersécurité. Dans le contexte des cybermenaces, la capacité d'action et l'intégrité de sa population, de son économie, de ses autorités et des organisations internationales basées sur son territoire sont garanties*. »[346]

547 Selon le Rapport explicatif du DDPS du 24 août 2022 sur la législation d'exécution relative à la LSI, la sécurité de l'information *absolue* ne peut pas être atteinte[347]. Face aux cybermenaces, il s'agit de réduire, au moyen de mesures de protection adaptées, la probabilité d'un cyberincident et, s'il se produit, ses conséquences.

548 Autrement dit, comme l'ont souligné plusieurs personnes interrogées, la sécurité de l'information a un coût et son niveau dépend en définitive de choix politiques en matière d'allocation des ressources.

549 Or, la tendance qui se dégage des interrogatoires menés par OA est que, jusqu'à la fuite de données Xplain de juin 2023, les ressources allouées à la sécurité de l'information au sein des Unités directement concernées étaient globalement insuffisantes.

550 La fonction de délégué à la sécurité informatique des unités administratives (« DSIO »)[348] illustre ce constat. Cette fonction était centrale dans l'architecture de sécurité de l'information de la Confédération selon le droit en vigueur jusqu'au 31 décembre 2023. Elle l'est toujours, avec une nouvelle dénomination[349], sous l'égide de la LSI et de l'OSI.

551 Or, au moment des interrogatoires de novembre-décembre 2023 et selon les déclarations des personnes interrogées à ce sujet :

- A fedpol, le DSIO était surchargé, mais deux postes supplémentaires avaient été demandés ou mis au concours.
- A l'OFJ, la fonction de DSIO ne représentait que 10% environ du cahier des charges d'une seule personne, ce qui était largement insuffisant.

[346] Cyberstratégie nationale CSN, avril 2023, p. 11.
[347] Rapport explicatif du DDPS sur la législation d'exécution relative à la loi sur la sécurité de l'information, 24 août 2022, SG-DDPS-251.2-35/1/6/8, p. 5.
[348] Art. 13 al. 5 et 14 aOPCy.
[349] Préposés à la sécurité de l'information des unités administratives (art. 37 OSI).

- A l'OFDF, la fonction de DSIO était occupée par deux personnes, ce qui était suffisant. Il était prévu d'augmenter ce nombre, à mesure que des ressources se libèreraient dans d'autres fonctions.
- Au Commandement des opérations, auquel la Police militaire est subordonnée, la fonction de DSIO était occupée par une personne, ce qui était suffisant, mais ne le serait certainement plus à l'avenir au regard de la stratégie Administration fédérale numérique.
- Au SEM, la fonction de DSIO était occupée par une personne, ce qui était juste suffisant et devrait être renforcé vu les changements législatifs à venir.

552 Ces constatations relatives aux DSIO ont été communiquées à l'Organe de coordination à mi-décembre 2023 et nous comprenons que des démarches ont été effectuées dans l'intervalle au sein des unités précitées pour augmenter les ressources allouées à l'actuelle fonction de préposé à la sécurité de l'information des unités administratives.

d) Dépendance des Unités directement concernées à l'égard de Xplain

553 De façon générale, l'enquête révèle une dépendance des Unités directement concernées à l'égard de Xplain au cours des années sous enquête.

554 Selon leur analyse et en substance, il n'existait pas d'alternative à Xplain[350]. Le fait que la Confédération n'avait pas la propriété intellectuelle des applications fournies par Xplain est régulièrement mentionné dans les formulaires justifiant le recours à une adjudication de gré à gré[351]. Il en va de même de l'argument selon lequel, en substance, à vouloir changer de fournisseur, il faudrait changer de système, ce qui entraînerait des difficultés techniques, des coûts disproportionnés et des retards[352]. Les autres arguments avancés sont le manque de connaissances des autres fournisseurs dans les secteurs d'activité des unités en comparaison avec Xplain[353], le manque de ressources dans les unités, par exemple pour la

[350] Voir par exemple : [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.84-106); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.79-82). [redacted] (AUD 03.10.09.108-[redacted](AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.47-57). [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4); [redacted] (AUD 03.10.09.6-16).

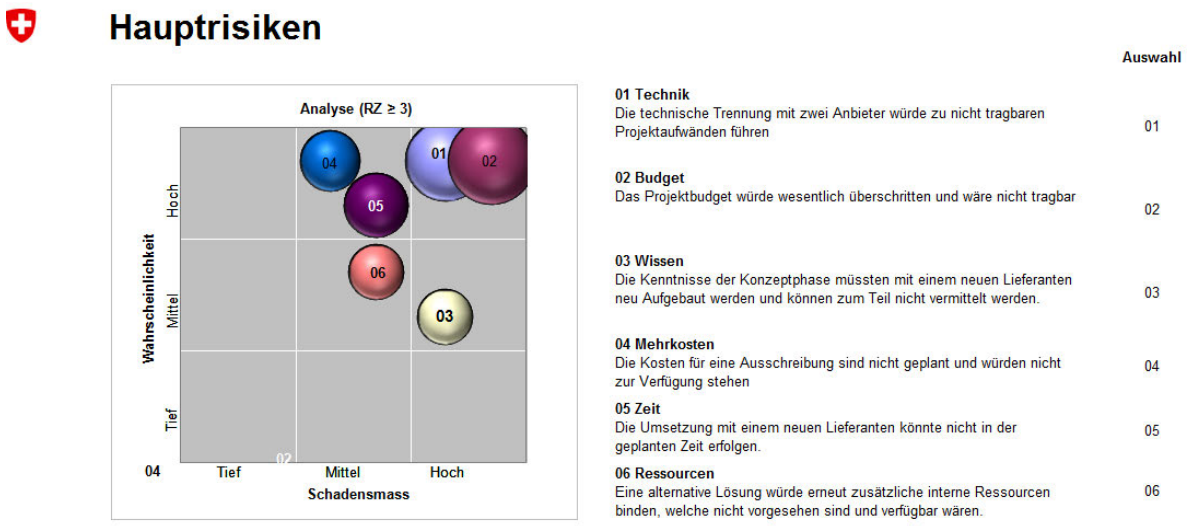
[351] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62) [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32). [redacted] (AUD 03.10.09.1-4); [redacted] (AUD 03.10.09.6-16).

[352] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.79-82). [redacted] (AUD 03.10.09.34-45) [redacted] (AUD 03.10.09.47-57). [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32) [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

[353] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

formation du personnel au nouveau système[354], ainsi que le coût et le temps supplémentaire qu'impliqueraient un nouvel appel d'offres[355].

555 A titre illustratif, le graphique suivant montre comment l'OFDF a pondéré différents risques liés au remplacement de Xplain par un nouveau fournisseur en fonction de leur probabilité et de l'ampleur des dommages potentiels[356] :



556 Les interrogatoires et l'examen de la correspondance électronique à notre disposition suggèrent que la dépendance avec Xplain a été identifiée par certaines Unités à tout le moins. Les conséquences à tirer du constat de dépendance à l'égard de ce fournisseur externe n'étaient en revanche pas évidentes.

557 Un projet de rapport interne à fedpol intitulé « *IKT-Beschaffungen fedpol PVS (Polizeisysteme im Bereich Bundeskriminalpolizei) – Aktuelle Situation* » du 26 juillet 2010 est illustratif à cet égard[357]. Selon sa page de garde, ce projet a été rédigé par un consultant externe à fedpol et il a été revu par un *Integrationsmanager* au sein de fedpol. Puis, le responsable de la section Systèmes de police II de fedpol a intégré le commentaire qui figure après la flèche[358] :

[354] [redacted] (AUD 03.10.09.18-23).

[355] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62). [redacted] (AUD 03.10.09.34-45) [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

[356] Extrait de EneXs Mobile: [redacted] (AUD 03.10.09.18-23). L'Organe d'enquête n'a pas identifié de version signée de ce document. Son caractère final ne fait toutefois pas de doute. Ce tableau figure en effet dans un document annexé à un e-mail de juin 2018 interne à l'OFCL dans lequel il est présenté comme « Final » (AUD 03.10.09.305).

[357] [redacted] (AUD 03.10.09.84-106).

[358] L'Organe d'enquête n'a pas identifié de version finale et signée de ce document.

Ausgehend von vorliegenden Liefer- und Dienstleistungsverträgen wird die Abhängigkeit von einer Lieferfirma augenfällig. Dies könnte für fedpol nicht nur beschaffungsrechtlich zunehmend problematisch sein (rechtskonforme Begründung) - sonder auch in einem höheren Risiko resultieren. ← **eine Abhängigkeit ist in jedem Fall und immer gegeben**. heute würde ich nicht wagen zu beurteilen, welche Abhängigkeit, die vom ISC oder die von Xplain problematischer ist. Der Bund hat viele solche Abhängigkeiten, weil sie schlicht weg nicht wegbedungen werden können (Oracle, Microsoft, HP, etc.). Wird die Anwendung ORMA durch eine andere ersetzt, so entsteht mit dem neuen Anbieter umgehend wieder ein gleiches Abhängigkeitspotenzial. Andererseits ist wirtschaftlich kaum vertretbar, dass auf dem Markt existierende Standardsoftware beim Bund nachgebaut werden. Dies selbst dann nicht, wenn der Markt für Standardsoftware im Polizeiumfeld nicht sehr gross ist.
Ich bitte beim Überarbeiten dieses Abschnittes meine Anmerkungen zu berücksichtigen. ¶

e) Relation fondée essentiellement sur la confiance

558 L'analyse des Données Exchange à notre disposition montre que la collaboration entre Xplain et les Unités directement concernées, ainsi que le CSI-DFJP, est le fait d'un cercle restreint d'employés de Xplain (une vingtaine au total ; en général entre deux et cinq par projet) qui est directement en contact avec un cercle relativement restreint d'employés des Unités directement concernées et du CSI-DFJP (en général entre une et trois personnes par projet).

559 Certaines de ces personnes ont été amenées à collaborer étroitement, sur une période de plusieurs années, dans le cadre des projets de développements confiés à Xplain ou dans le cadre du support fourni par cette dernière. Ces employés de Xplain étaient pour la plupart « *onboardés* », c'est-à-dire qu'ils disposaient d'un ordinateur portable, d'un compte utilisateur et d'un compte e-mail de la Confédération. Le tutoiement était utilisé avec ce fournisseur externe pratiquement sans exception par les employés des Unités directement concernées et du CSI-DFJSP. Les échanges par e-mails sont marqués par l'usage fréquent de surnoms.

560 En outre, un employé du SEM, mentionné comme personne clé dans un contrat en 2011[359], s'est récusé fin mai 2023 de tout dossier en lien avec Xplain au motif qu'une amitié s'était développée entre lui et l'un des fondateurs de Xplain lors de la collaboration avec son unité et que son fils faisait son apprentissage chez Xplain[360]. Il apparaît par ailleurs qu'une personne était employée par Xplain et désignée comme personne clé dans certains contrats avec fedpol[361], avant d'être employée par fedpol et désignée comme personne clé dans des contrats avec Xplain[362]. Enfin, dans le cas d'un employé de fedpol, des éléments découverts fortuitement par l'Organe d'enquête suggèrent que certains privilèges ont été demandés aux administrateurs de Xplain[363].

561 La correspondance entre les employés de Xplain et les employés de la Confédération en question imprime en définitive le sentiment d'une relation reposant essentiellement sur la confiance ; sur ce point, certaines personnes interrogées ont relevé que les employés de Xplain en question avaient passé avec

[359] AUD B03.04.08.48.
[360] AUD B03.04.08.67.
[361] AUD B03.04.10.237; AUD B03.04.10.208.
[362] AUD B03.04.10.383; AUD B03.04.10.715.
[363] Ces demandes portent sur des facilités éventuelles dont disposeraient les administrateurs de Xplain pour obtenir des billets de rencontres de football ou pour acquérir des billets d'avion Berne-Madrid à des tarifs préférentiels. Dans un cas, ce collaborateur de fedpol semble avoir sollicité un administrateur de Xplain pour une opportunité professionnelle éventuelle au sein de Xplain pour un membre de sa famille. OA a informé l'Organe de coordination à ce sujet le 28 février 2024 (cf. *supra* par. 29 ; AUD 01.04.23 ; B01.04.01 ; B01.04.02 ; B01.04.03 ; B01.04.04).

succès un contrôle de sécurité lié aux personnes (CSP), qu'ils s'étaient engagés à respecter les directives en matière de sécurité informatique et qu'ils étaient ainsi, en substance, soumis aux mêmes règles que les employés de la Confédération.

562 D'une part, si l'enquête a identifié plusieurs déclarations de sécurité relatives à des employés de Xplain, ainsi que des engagements à respecter les directives en matière de sécurité informatique, il n'a pas été possible de confirmer que ces déclarations et ces engagements ont été signés systématiquement par tous les employés de Xplain qui ont été « *onboardés* ».

563 D'autre part, les employés de Xplain n'en demeuraient pas moins des employés d'un fournisseur externe.

B. Recommandations

1. Sur le plan organisationnel

564 Au cours de l'enquête administrative, qui s'est déroulée entre le 1er septembre 2023 et le 28 mars 2024, l'organisation de la Confédération en matière de sécurité de l'information a connu un changement majeur.

565 La LSI et l'OSI sont en effet entrées en vigueur le 1er janvier 2024 au terme d'un processus initié avec le Message du Conseil fédéral de février 2017[364].

566 Depuis le 1er janvier 2024[365], la Confédération compte trois nouvelles unités administratives, au sein du DDPS : le Secrétariat d'État à la politique de sécurité (SEPOS), le Commandement Cyber (cdmt Cyber) et l'Office fédéral de la cybersécurité (OFCS). L'OFCS succède au NCSC et le cmdt Cyber succède à la BAC.

567 Les recommandations sur le plan organisationnel doivent donc tenir compte de l'organisation qui a été mise en place le 1er janvier 2024.

568 Selon l'Organe d'enquête, les résultats de la présente enquête administrative n'appellent pas une remise en cause des *principes* suivants de la LSI et de l'OSI :

i. Les autorités soumises à la LSI veillent, chacune dans son domaine de compétence, à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques[366].

ii. Chaque unité administrative est responsable de la protection des informations qu'elle traite ou dont elle délègue le traitement et de la sécurité des moyens informatiques qu'elle exploite elle-même ou fait exploiter par des tiers [367].

569 L'Organe d'enquête estime toutefois que cette responsabilité de principe des unités administratives devrait être tempérée à plusieurs égards.

570 En effet, la complexité de la sécurité de l'information et l'exigence d'efficience imposent à notre sens d'optimiser l'emploi des connaissances et des moyens existants (humains et techniques) en matière de sécurité de l'information, avant d'envisager d'éventuels moyens supplémentaires.

571 Or, il résulte des interrogatoires menés dans la présente enquête que ces connaissances et ces moyens se trouvaient, avant le 31 décembre 2023, *essentiellement* chez les fournisseurs internes de prestations

[364] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765.
[365] RO 2023 746.
[366] Art. 7 LSI ; art. 3 OSI.
[367] Art. 4 al. 1 OSI.

informatiques (OFIT, BAC, unité informatique du DFAE, CSI-DFJP), d'une part, et au sein du NCSC, d'autre part.

572 L'enquête a montré que les autres unités administratives touchées par l'enquête disposaient, en matière de sécurité de l'information, de compétences et de moyens inégaux, mais dans tous les cas moindres que ceux des fournisseurs internes précités et du NCSC.

573 En outre et dans le prolongement de ce constat, l'Organe d'enquête note que, dans le système actuel de la LSI et de l'OSI, *responsabilité* et *connaissances* en matière de sécurité de l'information sont, au moins en partie, décorrélées. Les interrogatoires dans la présente enquête administrative ont ainsi mis en lumière un décalage entre (i) la responsabilité des unités administratives prévue par l'art. 4 OSI et (ii) les informations dont elles disposent pour assurer la sécurité de l'information (et donc assumer la responsabilité qui leur est allouée par l'art. 4 OSI).

574 Il est vrai que l'art. 30 al. 2 OSI prévoit que les fournisseurs internes de prestations informatiques mettent à la disposition des unités administratives les informations dont elles ont besoin pour assurer la sécurité de l'information. L'existence même de cette règle tend à confirmer le constat fait lors des interrogatoires selon lequel les fournisseurs internes de prestations informatiques disposent d'informations que les unités administratives *n'ont pas* et qu'elles doivent donc leur transmettre. Toutefois, d'après l'Organe d'enquête, ces connaissances plus étendues devraient s'accompagner d'une responsabilité plus étendue. La mise en œuvre concrète de cette recommandation appelle des travaux qui dépassent le cadre de la présente enquête administrative.

575 Enfin, l'enquête a révélé qu'après qu'une unité administrative a identifié une fonctionnalité (« *Error Reporting* ») conduisant potentiellement à des flux de données productives dans le cadre de demandes de support, l'information n'apparaît pas avoir circulé entre les Unités directement concernées. Cela illustre à notre sens les risques de la décentralisation en matière de sécurité de l'information.

576 Ces constats sont à l'origine des recommandations suivantes.

Recommandations :

1. Prévoir une responsabilité accrue des fournisseurs internes de prestations informatiques en matière de sécurité de l'information lorsqu'ils exploitent des moyens informatiques ou traitent des informations pour les bénéficiaires de leurs prestations.

2. Renforcer la centralisation des compétences en matière de sécurité de l'information de la Confédération :

   a) Confier au SEPOS la responsabilité du pilotage et de la surveillance de la sécurité de l'information de la Confédération, qui appartient actuellement aux départements (comparer art. 39 OSI).

   b) Attribuer au SEPOS des délégués soumis au pouvoir d'instruction du SEPOS et qui seraient détachés dans les unités administratives et les départements, afin de trouver un équilibre entre (i) la centralisation des compétences et des moyens en matière de sécurité de l'information et (ii) la nécessité de prendre en compte les spécificités et besoins individuels des unités administratives et des départements.

3. Le SEPOS et l'OFCS devraient clarifier rapidement et clairement la répartition de leur rôle respectif au regard des art. 8 al. 2, 10 al. 3, 21 al. 2 let. a et 43 al. 2 OSI.

2. Sur le fond

577 Les enseignements tirés de la présente enquête administrative appellent à notre sens également des recommandations sur le fond.

578 Comme le relevait le Conseil fédéral en 2017 à l'occasion du message concernant la LSI, « *[l]a sécurité des moyens informatiques est souvent considérée comme une affaire technique, ce qui n'est vrai que dans une faible mesure : la majorité des mesures de sécurité informatique sont en effet de nature organisationnelle* »[368]. La majorité de nos recommandations sont également de cette nature.

579 Les recommandations de nature technique qui figurent ci-dessous sont technologiquement neutres.

Recommandations :

1. Des ressources suffisantes devraient être allouées aux autorités et organisations soumises à la LSI et à la LPD pour mener leurs tâches en matière de sécurité de l'information et de protection des données.

2. Chaque unité administrative doit connaître ses fournisseurs externes et le SEPOS doit connaître l'identité et la criticité de tous les fournisseurs externes.

3. La culture de sécurité de l'information et de protection des données doit être renforcée (sensibilisation et formation), en particulier parmi les personnes appelées à traiter des données des systèmes de production de la Confédération.

4. L'interdiction de *transférer* des données productives à des fournisseurs externes devrait être claire et clairement communiquée.

5. Le fait qu'une personne physique est un fournisseur externe ou qu'elle est employée ou organe d'un fournisseur externe devrait être rendu immédiatement reconnaissable par le personnel de la Confédération.

6. *L'accès* par des fournisseurs externes à des données productives, sur site ou à distance, devrait être réduit au minimum, strictement encadré et contrôlé (mise en œuvre de processus écrits, uniformes et revus régulièrement, reposant sur le principe des quatre yeux et non sur la confiance).

7. L'effacement des données productives qui ont par le passé été mises à disposition de fournisseurs externes actuels ou passés de la Confédération doit être systématiquement demandé et sa mise en œuvre vérifiée (y compris archives).

8. Les traitements de données à l'étranger par des fournisseurs externes doivent être identifiés et, le cas échéant, encadrés.

[368] Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 2765 2791.

9. Les applications devraient concilier sécurité et protection des données dès la conception (« *privacy and security by design* ») et facilité d'utilisation (« *user friendliness* »).

10. La mise en place de limitations techniques visant à prévenir les transferts de données productives devrait être examinée pour certaines situations, selon la criticité des données en cause.

* * *