Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

**Office fédéral de la justice OFJ**
Domaine de direction Droit public
Unité Projets législatifs I

30 avril 2024

# Evaluation de l'adéquation - Etats-Unis

## Etablissement d'un cadre pour le transfert de données personnelles depuis la Suisse vers les organisations certifiées aux Etats-Unis (*Swiss-U.S. Data Privacy Framework*) - Evaluation de l'adéquation du niveau de protection des données personnelles

BJ-D-AED93401/290

**Table des matières**

# 1 Contexte

## 1.1 Régime d'adéquation introduit par la loi du 25 septembre 2020 sur la protection des données

La nouvelle législation en matière de protection des données en vigueur depuis le 1er septembre 2023 a introduit un changement de compétence : en vertu de l'art. 16, al. 1, de la loi du 25 septembre 2020 sur la protection des données (LPD)[1] ainsi que de l'art. 8, al. 1, de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[2] le Conseil fédéral est chargé de déterminer si un Etat, un territoire, un secteur déterminé dans un Etat ou un organisme international garantit un niveau de protection adéquat des données. L'annexe 1 OPDo contient une liste des Etats, territoires, secteurs déterminés dans un Etat et organismes internationaux dans lesquels un niveau de protection adéquat des données est garanti.

Par ailleurs, la tâche d'évaluer le caractère adéquat du niveau de protection des données incombe à l'Office fédéral de la justice[3]; il s'agit d'une évaluation de nature juridique qui est publiée.

## 1.2 Précédent cadre et invalidation

Sous le régime de la loi du 19 juin 1992 sur la protection des données (abrogée), le Préposé fédéral à la protection des données et à la transparence (PFPDT) tenait une liste indicative des Etats qui offraient un niveau de protection adéquat des données.

Le 11 janvier 2017, le PFPDT avait ajouté les Etats-Unis sur sa liste des Etats pour les échanges de données avec les entreprises certifiées dans le cadre du *Swiss-U.S. Privacy Shield*. L'UE était au bénéfice d'un cadre pratiquement identique avec les Etats-Unis.

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a rendu une décision dans le cadre de l'affaire dite Schrems II (Affaire C-311/18), jugeant la protection accordée comme insuffisante et ainsi invalidant le mécanisme de transmission de données personnelles de l'UE vers les Etats-Unis, au motif que celui-ci permettait des dérogations disproportionnées à la protection des données en vue de la surveillance par les services de renseignement des Etats-Unis et n'offrait aucun recours effectif aux personnes concernées.

Même si la décision de la CJUE n'a pas d'effet contraignant pour la Suisse, en considération du principe général de l'Etat de droit ainsi que du besoin de sécurité juridique et prenant en compte que le cadre régissant les échanges de données personnelles entre la Suisse et les Etats-Unis était quasiment identique au cadre entre l'UE et les Etats-Unis, le PFPDT a estimé qu'il était fondé à réexaminer la présence des États-Unis dans la liste indicative des États garantissant un niveau de protection adéquat qu'il tenait. Le PFPDT a publié le 8 septembre 2020 une prise de position dans laquelle il a considéré que les États-Unis ne répondaient pas

---

1 RS 235.1.

2 RS 235.11.

3 Conformément à l'art. 7, al. 1, lit. d de l'ordonnance du 17 novembre 1999 sur l'organisation du département fédéral de justice et police (RS 172.213.1), cette tâche est exercée en collaboration avec d'autres offices compétents.

aux exigences d'une protection adéquate des données au sens de la loi sur la protection des données et a retiré les Etats-Unis de sa liste. De ce fait, le Conseil fédéral n'a pas inclus les Etats-Unis dans la liste des Etats de l'annexe 1 OPDo au moment de l'entrée en vigueur de la nouvelle législation le 1er septembre 2023.

### 1.3 Etablissement d'un cadre pour le transfert de données personnelles depuis la Suisse vers les organisations certifiées aux Etats-Unis

Suite au retrait du précédent cadre entre les Etats-Unis et la Suisse de la liste du PFPDT, des discussions ont eu lieu entre les Etats-Unis et la Suisse, en parallèle aux discussions menées entre les Etats-Unis et l'Union européenne.

Ces discussions ont abouti à l'établissement d'un cadre commercial pour les organisations certifiées (principes, y compris principes supplémentaires, du cadre entre la Suisse et les États-Unis sur la protection des données), à la publication de différents documents par le gouvernement des Etats-Unis ainsi que par les autorités compétentes aux Etats-Unis (décret exécutif 14086 du 7 octobre 2022, règlement sur la cour d'examen en matière de protection des données du procureur général des États-Unis publié le 7 octobre 2022, directive 126 de la communauté du renseignement établie par le bureau de la directrice du renseignement national (ODNI) le 6 décembre 2022), à la désignation de la Suisse le 7 juin 2024 en tant qu'Etat bénéficiant du mécanisme de recours à deux niveaux comprenant l'accès à la cour d'examen en matière de protection des données ainsi qu'à la remise de lettres des autorités compétentes aux Etats-Unis visant à confirmer les engagements pris. L'ensemble de ces documents[4], accessibles au moyen des liens vers les textes de référence inclus en fin de document, constitue le cadre pour le transfert de données personnelles depuis la Suisse vers les organisations certifiées aux Etats-Unis (*Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)*).

L'examen ci-dessous vise à évaluer si l'ensemble de ces documents permet aux Etats-Unis de garantir un niveau de protection adéquat pour les transferts de données personnelles entre responsables du traitement ou sous-traitants en Suisse et organisations certifiées aux Etats-Unis, en application des critères d'évaluation fixés par l'OPDo.

## 2 Critères d'évaluation de l'adéquation

L'art. 8 OPDo définit plusieurs critères qui doivent être en particulier pris en compte dans les évaluations, à savoir :

a) les engagements internationaux de l'Etat ou de l'organisme international, notamment en matière de protection des données ;
b) l'état de droit et le respect des droits de l'homme ;
c) la législation applicable, notamment en matière de protection des données, de même que sa mise en œuvre et la jurisprudence y relative ;
d) la garantie effective des droits des personnes concernées et des voies de droit ;

[4] Ces documents ne sont disponibles qu'en anglais.

e) le fonctionnement effectif d'une ou de plusieurs autorités indépendantes chargées de la protection des données dans l'État concerné, ou auxquelles un organisme international est soumis, et disposant de pouvoirs et de compétences suffisants.

L'annexe 1 OPDo contient la liste des Etats, territoires, secteurs déterminés dans un Etat et organismes internationaux dans lesquels un niveau de protection adéquat des données est garanti. Cette liste a force obligatoire.

Par niveau de protection adéquat, il est entendu un niveau de protection essentiellement équivalent à celui assuré par le droit suisse de la protection des données. Il ne s'agit pas de comparer point par point les systèmes prévus mais de déterminer si, dans son ensemble, le régime prévu par un Etat, un territoire, un secteur déterminé dans un Etat ou un organisme international assure un niveau de protection essentiellement équivalent de par le contenu des droits à la vie privée garantis, la mise en œuvre de ces droits ainsi que les moyens de contrôle employés. Il y a lieu dans ce contexte de prendre en compte les différences de traditions juridiques et culturelles entre un Etat, un territoire, un secteur déterminé dans un Etat ou un organisme international faisant l'objet d'une évaluation de l'adéquation et la Suisse.

L'UE utilise des critères très similaires dans le cadre de l'évaluation de l'adéquation du niveau de protection des données personnelles d'Etats tiers conformément à l'article 45 du Règlement général sur la protection des données[5].

## 3 Cadre commercial pour les transferts de données personnelles entre responsables du traitement ou sous-traitants en Suisse et organisations certifiées aux Etats-Unis

### 3.1 Législation applicable

#### 3.1.1 Principes du cadre

Les principes, y compris les principes supplémentaires, du cadre pour le transfert de données personnelles depuis la Suisse vers les organisations certifiées aux Etats-Unis (ci-après: les principes du *Swiss-U.S. DPF* ou les principes)[6], sont basés sur un système de certification par lequel les organisations, soit les entreprises, des Etats-Unis qui désirent bénéficier du cadre pour le transfert de données personnelles s'engagent à respecter un ensemble de principes de protection de la vie privée. Pour pouvoir être certifiée au titre du *Swiss-U.S. DPF*, une organisation doit être soumise aux pouvoirs d'enquête et d'exécution de la Commission fédérale du commerce ou du Département des transports ; par ailleurs, elle doit certifier son adhésion aux principes chaque année.

Les principes du *Swiss-U.S. DPF* définissent les données personnelles comme les données concernant une personne identifiée ou identifiable qui relèvent du champ d'application de la LPD et de ses ordonnances, reçues par une organisation aux États-Unis en provenance de

---

[5] C.f. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1, accessible sous le lien suivant: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu).

[6] C.f. liens vers les textes de référence en fin de document.

Suisse et enregistrées sous quelque forme que ce soit. De même, la notion de traitement est définie par les principes comme toute opération ou tout ensemble d'opérations appliqué(s) à des données personnelles et effectuée(s) ou non à l'aide de procédés automatisés, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication ou la diffusion ainsi que l'effacement ou la destruction. Ces notions importantes sont dès lors définies de la même manière qu'en droit suisse.

Les principes du *Swiss-U.S. DPF* garantissent le respect des principes essentiels applicables en droit suisse de la protection des données, définis notamment par l'art. 6 LPD.

Ainsi les données personnelles doivent être traitées de manière licite et proportionnelle, collectées pour des finalités déterminées et utilisées ultérieurement de manière compatible avec les finalités du traitement. Dans le cadre du *Swiss-U.S. DPF*, cela ressort principalement du principe d'intégrité des données et de limitation de la finalité (*Data Integrity and Purpose Limitation Principle*), mais également du principe du libre-choix (*Choice Principle*), dès lors qu'une organisation doit offrir aux personnes concernées la possibilité de déterminer si leurs données personnelles peuvent être divulguées à un tiers ou utilisées pour une finalité qui diffère sensiblement de celle pour laquelle elles ont été initialement collectées ou ultérieurement autorisées par ces personnes.

Les données personnelles doivent être exactes et traitées de manière proportionnelle au regard des finalités pour lesquelles elles sont traitées ; par ailleurs, elles ne doivent pas être conservées pendant une durée qui excède celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Dans le cadre du *Swiss-U.S. DPF*, cela ressort des principes d'intégrité des données et de limitation de la finalité ainsi que du libre-choix.

La sécurité des données doit être garantie : les responsables du traitement et les sous-traitants doivent prendre des mesures de sécurité raisonnables et appropriées compte tenu des risques présentés par le traitement et de la nature des données traitées. Dans le cadre du *Swiss-U.S. DPF*, cela ressort du principe de sécurité (S*ecurity Principle*).

Conformément au principe de transparence, les personnes concernées doivent être informées des principales caractéristiques du traitement de leurs données personnelles : les organisations doivent notamment informer les personnes concernées de la participation au *Swiss-U.S. DPF*, du type de données collectées, de la finalité du traitement, de leurs droits et des voies de droit disponibles. Dans le cadre du *Swiss-U.S. DPF*, cela ressort du principe d'information (*Notice Principle*). Les organisations doivent rendre publiques leurs règles en matière de protection de la vie privée reflétant les principes du *Swiss-U.S. DPF*.

Les personnes concernées disposent de certains droits opposables au responsable du traitement ou au sous-traitant, en particulier le droit d'accès aux données, le droit de s'opposer au traitement et le droit de faire rectifier et effacer les données. Ainsi les personnes concernées ont le droit, sans avoir à se justifier, d'obtenir la confirmation que des données personnelles les concernant sont traitées, la communication de ces données et des informations sur la finalité du traitement, les catégories de données personnelles traitées et les destinataires auxquels les données sont communiquées. Le droit d'accès ne peut être limité que dans des circonstances exceptionnelles similaires à celles prévues en droit suisse, p.ex. lorsque les intérêts prépondérants d'un tiers l'exigent. En outre, les personnes concernées ont le droit d'obtenir la rectification des données inexactes et la suppression des données qui ont été

traitées en violation des principes applicables. Dans le cadre du *Swiss-U.S. DPF*, cela ressort du principe d'accès (*Access Principle, Supplementary Principle on Access*).

Des règles spécifiques s'appliquent aux transferts ultérieurs de données personnelles entre une organisation certifiée et un tiers responsable du traitement ou sous-traitant conformément au principe de responsabilité pour les transferts ultérieurs (*Accountability for Onward Transfer Principle*). Un transfert ultérieur ne peut avoir lieu qu'à des fins délimitées et spécifiques, sur la base d'un contrat et uniquement si ledit contrat exige du tiers qu'il fournisse le même niveau de protection que celui garanti par les principes.

En vertu du principe de recours, application et responsabilité (*Recourse, Enforcement and Liability Principle*), les organisations certifiées doivent mettre en place des mécanismes efficaces pour garantir le respect des principes. Les organisations doivent également prendre des mesures pour vérifier que leurs politiques de protection de la vie privée sont conformes aux principes et qu'elles sont effectivement respectées. Cela peut se faire soit par un système d'auto-évaluation, soit par des contrôles de conformité externes.

Par ailleurs, des garanties spécifiques s'appliquent pour l'utilisation de données sensibles au sens du droit suisse : les organisations doivent obtenir le consentement exprès des personnes concernées pour divulguer ces données à un tiers ou utiliser ces données pour des finalités autres que celles pour lesquelles elles ont été collectées ou autorisées ultérieurement par ces personnes dans le cadre de l'exercice de leur choix (*opt-in*). Il n'est toutefois pas nécessaire d'obtenir ce consentement dans certaines circonstances limitées, de manière similaire aux exceptions prévues en droit suisse, par exemple lorsque les intérêts prépondérants d'un tiers l'exigent. Dans le cadre du *Swiss-U.S. DPF*, cela ressort du principe du choix ainsi que du principe supplémentaire sur les données sensibles (*Supplementary Principle on Sensitive Data)*.

### 3.1.2 Champ d'application

Le cadre commercial est applicable aux données personnelles[7] transférées depuis la Suisse vers des organisations aux Etats-Unis qui ont certifié leur adhésion aux principes (c.f. 3.1.1. ci-dessus).

Il est applicable aux organisations aux Etats-Unis qualifiées de responsables du traitement au sens de l'art. 5 lit. j LPD ou de sous-traitants au sens de l'art. 5 lit. k LPD. Les sous-traitants doivent être contractuellement tenus de n'agir que sur instruction du responsable du traitement en Suisse et d'aider ce dernier à répondre aux personnes qui exercent leurs droits en vertu des principes.

[7] Font exception les données collectées pour la publication, la diffusion ou d'autres formes de communication publique de matériel journalistique et les informations contenues dans du matériel déjà publié et diffusé à partir d'archives médiatiques.

### 3.2 Garanties effectives, autorité indépendante, voies de droit

#### 3.2.1 Gestion du cadre commercial, certification et surveillance

La gestion du cadre commercial est assurée par le Département du commerce des Etats-Unis (DoC).

Pour obtenir une auto-certification initiale ou le renouvellement d'une auto-certification (base annuelle) au titre du *Swiss-U.S. DPF*, les organisations sont tenues de déclarer publiquement leur engagement à respecter les principes ainsi qu'à mettre à disposition leurs politiques de protection de la vie privée et à les mettre pleinement en œuvre. Les organisations doivent également transmettre au DoC des informations notamment concernant les finalités pour lesquelles des données personnelles seront traitées, le mécanisme de recours indépendant pertinent et l'organe statutaire compétent pour assurer le respect des principes. Les organisations qui s'auto-certifient pour la première fois ne sont pas autorisées à faire publiquement référence à leur adhésion aux principes avant que le DoC n'ait ajouté l'organisation à la liste des organisations participantes, qui est tenue à jour et mise à la disposition du public par le DoC.

Le DoC a également une fonction de surveillance. Pour garantir la bonne application du *Swiss-U.S. DPF*, le DoC tiendra à jour et mettra à la disposition du public la liste des organisations qui se sont auto-certifiées auprès du DoC et ont déclaré leur engagement à adhérer aux principes afin que ces dernières puissent être identifiées comme telles ainsi qu'un registre des organisations qui ont été retirées de la liste, en précisant dans chaque cas la raison de ce retrait. Le DoC retirera de la liste les organisations qui se retirent volontairement du *Swiss-U.S. DPF* ou qui ne procèdent pas au renouvellement de leur certification annuelle auprès du DoC ; ces organisations doivent soit continuer à appliquer les principes aux données personnelles qu'elles ont reçues dans le cadre du *Swiss-U.S. DPF* et réitérer au DoC chaque année leur engagement à le faire (tant qu'elles conservent ces données), soit assurer une protection appropriée des données personnelles par un autre moyen autorisé (par exemple en utilisant un contrat qui reflète intégralement les exigences des clauses contractuelles types pertinentes approuvées, établies ou reconnues par le PFPDT), soit à restituer ou à supprimer les données. Le DoC retirera également de la liste les organisations qui n'ont pas constamment respecté les principes ; ces organisations doivent restituer ou supprimer les données personnelles qu'elles ont reçues dans le cadre du *Swiss-U.S. DPF*.

Le DoC est chargé d'effectuer des contrôles pour vérifier que les exigences de certification sont remplies, en particulier que les principes sont effectivement respectés. Il effectuera des contrôles ponctuels auprès d'organisations sélectionnées de manière aléatoire et également auprès d'organisations spécifiques lorsque des problèmes potentiels sont identifiés, notamment si le DoC reçoit des plaintes ou si l'organisation ne répond pas de manière satisfaisante aux demandes de renseignements. Dans certains cas, l'organisation peut être renvoyée à l'autorité compétente en vue d'une éventuelle action coercitive.

Le DoC exercera un contrôle afin de s'assurer qu'il n'y ait pas de fausse déclaration d'adhésion aux principes, notamment s'agissant des organisations qui sont retirées de la liste. Le cas échéant, il pourra renvoyer l'affaire à l'autorité compétente en vue d'une éventuelle action coercitive.

### 3.2.2 Garantie de l'application du cadre

Pour pouvoir participer au cadre commercial, les organisations doivent être soumises à la juridiction des autorités compétentes aux Etats-Unis, à savoir la Commission fédérale du commerce (FTC) ou le Département des transports (DoT). Ces autorités disposent de pouvoirs d'enquête et d'exécution permettant de garantir efficacement le respect des principes[8].

La FTC est une autorité composée de cinq commissaires nommés par le président des Etats-Unis ; la nomination doit ensuite être confirmée par le Sénat. Les commissaires, qui ne sont pas autorisés à exercer une autre activité ou un autre emploi durant leur mandat de sept ans, ne peuvent être révoqués par le président que pour de justes motifs. La FTC a pour mission de protéger le public des pratiques commerciales trompeuses ou déloyales et des méthodes de concurrence déloyale. Elle peut enquêter sur le respect des principes ainsi que sur les fausses déclarations d'adhésion au cadre commercial. La FTC peut requérir des décisions administratives ou des décisions de tribunaux fédéraux ; elle peut contrôler le respect de ces décisions en contraignant les organisations à produire des documents et peut recourir au système judiciaire pour faire appliquer ces décisions en cas de non-respect.

Le DoT est seul compétent pour réglementer les pratiques des compagnies aériennes en matière de protection de la vie privée ; dans le cas des pratiques des agences de voyage liées au transport aérien ou à la vente de services de transport aérien, cette compétence est partagée avec la FTC. Si un règlement du litige n'est pas possible, le DoT peut demander à un juge administratif du DoT indépendant et impartial d'émettre des ordonnances de cessation et d'abstention ou d'imposer des sanctions de nature civile, ou peut demander la même réparation devant les tribunaux des Etats-Unis[9]. Le DoT s'est par ailleurs engagé à donner la priorité aux enquêtes relatives à des violations présumées des principes, prendre les mesures d'exécution appropriées en cas de fausse déclarations d'adhésion au cadre commercial et assurer le suivi et la publication des ordonnances d'exécution relatives à ce cadre.

Au vu de ce qui précède, la FTC et le DoT peuvent être qualifiées d'autorités de contrôle indépendantes dotées de pouvoirs et de compétences suffisants dans la perspective de la garantie d'un niveau de protection adéquat des données personnelles.

### 3.2.3 Voies de droit

Dans le cadre de leur certification, les organisations doivent satisfaire aux exigences du principe de recours, application et responsabilité (c.f. ch. 3.1.1.) en prévoyant des mécanismes de recours indépendants, efficaces et facilement accessibles, en vue de la résolution rapide des litiges sans frais pour la personne concernée.

Les organisations peuvent choisir des mécanismes de recours indépendants en Suisse ou aux Etats-Unis et peuvent opter pour des programmes de protection de la vie privée élaborés par le secteur privé et qui intègrent les principes dans leurs réglementations, des autorités de

---

[8] C.f. lettres de la FTC et du DoT, accessibles au moyen des liens vers les textes de référence en fin de document.

[9] C.f. titre 49 du Code des Etats-Unis, réglementation relative aux transports, accessible sous le lien suivant : 49 USC Ch. 461: INVESTIGATIONS AND PROCEEDINGS (house.gov).

surveillance légales ou réglementaires prévoyant le traitement des plaintes individuelles et le règlement des différends ou un engagement à coopérer avec le PFPDT.

Les personnes concernées peuvent déposer une plainte directement auprès d'une organisation, auprès d'un organisme indépendant de règlement des litiges désigné par l'organisation ou auprès du PFPDT. Le DoC renverra les organisations qui ne parviennent pas à résoudre un litige à la FTC et au DoT. La FTC et le DoT examineront en priorité les cas de non-respect des principes signalés par le DoC et le PFPDT. Les personnes concernées peuvent également déposer des plaintes directement auprès de la FTC par l'intermédiaire de la base de données *Consumer Sentinel* et peuvent utiliser le site web du DoT pour déposer directement des plaintes relatives à la protection de la vie privée contre les compagnies aériennes et les agents de billetterie.

Tant les organisations que les mécanismes de recours indépendants responsables sont tenus de répondre rapidement aux plaintes. Si une organisation ne se conforme pas à la décision d'un organisme indépendant de règlement des litiges ou d'un organisme gouvernemental, cela peut aboutir à la radiation de la liste tenue à jour et mise à la disposition du public par le DoC.

Les personnes concernées peuvent également porter plainte auprès du PFPDT. Par ailleurs et afin d'accélérer le traitement des plaintes, un point de contact auprès du DoC est en liaison directe avec le PFPDT. Cela permet aux personnes concernées de déposer des plaintes directement auprès du PFDPT et de les faire transmettre au DoC en tant qu'autorité chargée de l'administration du cadre commercial ; cela peut notamment aboutir à la radiation de la liste tenue à jour et mise à la disposition du public par le DoC.

Si la plainte d'une personne concernée n'a pas été résolue par l'un des mécanismes évoqués ci-dessus, la personne concernée peut, sous certaines conditions, invoquer l'option d'arbitrage contraignant décrite à l'annexe I des principes. Selon cette option qui ne peut intervenir qu'en dernier recours, un panel d'arbitrage composé d'un ou de trois arbitres (selon le souhait des parties) a le pouvoir d'imposer des mesures individuelles de réparation non-pécuniaires telles que l'accès, la correction, la suppression ou la restitution des données personnelles. Une liste d'arbitres sera définie conjointement par le DoC et la Suisse sur la base de leur indépendance, de leur intégrité et de leur expérience. Le Centre international pour le règlement des différends (*International Center for Dispute Resolution,* ICDR) de l'Association américaine d'arbitrage[10] administrera les litiges. La procédure devant un panel d'arbitrage est régie par un ensemble de règles d'arbitrage convenues et un code de conduite pour les arbitres. L'application des sentences arbitrales prononcées peut être requise devant les tribunaux aux Etats-Unis[11].

Ainsi la garantie des voies de droit est assurée dès lors que les voies de droit décrites ci-dessus permettent d'assurer que les plaintes relatives au non-respect des principes du *Swiss-*

[10] Le site Internet de ce centre fournira des informations claires et concises sur le mécanisme d'arbitrage et la procédure de demande d'arbitrage lorsque le cadre commercial entrera en vigueur : International Centre for Dispute Resolution | ICDR.org.

[11] C.f. titre 9 du Code des Etats-Unis (*US Code*), réglementation relative à l'arbitrage, accessible sous le lien suivant : ARBITRATION (house.gov)

*U.S. DPF* par des organisations certifiées feront l'objet de décisions et de mécanismes de réparation efficaces.

# 4 Accès aux données personnelles transférées depuis la Suisse par les autorités publiques aux Etats-Unis

## 4.1 Accès à des fins d'application du droit pénal

### 4.1.1 Législation applicable, garanties effectives

La Constitution des Etats-Unis garantit que les autorités publiques ne disposent pas d'un pouvoir illimité ou arbitraire pour saisir des données personnelles. Le quatrième amendement[12] a pour objectif de protéger la vie privée et la sécurité des personnes contre les invasions arbitraires par des agents du gouvernement. Les normes relatives à la délivrance d'un mandat s'appliquent tant dans les cas de perquisitions et saisies physiques que de saisies de contenus stockés électroniquement. Même lorsqu'un mandat n'est pas requis, l'activité du gouvernement doit revêtir un caractère raisonnable conformément au quatrième amendement.

Les données personnelles traitées par des organisations certifiées peuvent être consultées à des fins d'application du droit pénal (*criminal law enforcement*), c'est-à-dire à des fins de répression pénale, par les procureurs fédéraux (*federal prosecutors*)[13] et les agents d'enquête fédéraux (*federal investigative agents*)[14] selon les procédures décrites ci-après. Il sied de préciser que ces procédures sont applicables indépendamment de la nationalité ou du lieu de résidence des personnes concernées.

Une citation à comparaître peut être délivrée par un grand jury dans le cadre d'enquêtes pénales relatives à certaines infractions graves, généralement à la demande d'un procureur fédéral, afin d'obliger une personne à produire ou mettre à disposition des documents commerciaux, des informations stockées électroniquement ou d'autres éléments tangibles[15]. En outre, l'utilisation de citations administratives peut être autorisée pour produire ou mettre à disposition des documents professionnels, des informations stockées électroniquement ou d'autres éléments tangibles dans le cadre d'enquêtes portant sur la fraude aux soins de santé, la maltraitance des enfants, la protection des services secrets, les affaires de substances contrôlées et les enquêtes de l'inspecteur général. Dans les deux cas, les informations doivent être pertinentes pour l'enquête et la citation doit être raisonnable, c'est-à-dire

---

[12] C.f. texte de la Constitution des Etats-Unis, accessible sous le lien suivant : U.S. Senate: Constitution of the United States.

[13] Les procureurs fédéraux sont des agents du Département de la justice.

[14] Les agents d'enquête fédéraux sont affiliés au Bureau fédéral d'enquête (FBI), qui est intégré au Département de la justice.

[15] C.f. Règles fédérales de procédure pénale (*Federal Rules of Criminal Procedure*), accessible sous le lien suivant : Current Rules of Practice & Procedure | United States Courts (uscourts.gov).

qu'elle ne doit pas être excessive, oppressive ou contraignante ; la citation peut d'ailleurs être contestée par son destinataire pour ces motifs.

Par ailleurs, des dispositions légales[16] permettent aux autorités chargées de l'application du droit pénal d'obtenir l'accès aux données de communication. Un tribunal peut émettre une ordonnance autorisant la collecte en temps réel, sans contenu, d'informations relatives à la numérotation, au routage, à l'adressage et à la signalisation d'un numéro de téléphone ou d'un courrier électronique sur certification que les informations susceptibles d'être obtenues sont pertinentes dans le cadre d'une enquête pénale en cours. L'utilisation de dispositifs de traçage peut être autorisée pour une période maximale de soixante jours, qui ne peut être prolongée que par une nouvelle décision de justice. En outre, l'accès aux informations sur les abonnés, aux données relatives au trafic et au contenu stocké des communications détenues par les fournisseurs de services internet, les compagnies de téléphone et d'autres fournisseurs de services peut être obtenu sur la base d'un mandat d'un juge fondé sur la présomption que le compte en question contient des preuves d'une infraction. Pour les informations relatives à l'inscription des abonnés, aux adresses IP et à la facturation, les autorités chargées de l'application du droit pénal peuvent obtenir une citation à comparaître. Pour la plupart des autres informations stockées sans contenu, une ordonnance du tribunal pourra être émise si le juge est convaincu que les informations demandées sont pertinentes et importantes pour une enquête pénale en cours.

Les autorités chargées de l'application du droit pénal peuvent également intercepter en temps réel des communications filaires, orales ou électroniques sur la base d'une ordonnance judiciaire dans laquelle un juge constate, entre autres, qu'il existe une présomption que la mise sur écoute ou l'interception électronique produira des preuves d'une infraction ou de l'endroit où se trouve un fugitif.

S'il existe une présomption que des objets saisissables sont susceptibles d'être trouvés, par exemple à titre de preuve d'une infraction, un juge peut délivrer un mandat de perquisition ou de saisie. Toutefois, la personne concernée peut demander la suppression des preuves obtenues illégalement par ce moyen si celles-ci sont présentées au cours d'une procédure pénale. Par ailleurs, lorsqu'un détenteur de données, par exemple une entreprise certifiée, est tenu de divulguer des données en vertu d'un mandat, il peut notamment contester l'obligation de divulgation au motif qu'elle constitue une contrainte indue[17].

Outre le cadre fixé par les dispositions légales susmentionnées pour l'accès aux données par les autorités publiques fédérales à des fins d'application du droit pénal, le procureur général des Etats-Unis (*Advocate General*) a publié des lignes directrices qui imposent des limites supplémentaires à l'accès et qui contiennent également des clauses de protection de la vie

---

[16] C.f. titre 18 du Code des Etats-Unis, réglementation relative aux infractions et à la procédure pénale (notamment les articles 2510ss, 2701ss et 3121ss), accessible sous le lien suivant : OLRC Home (house.gov).

[17] C.f. Règles fédérales de procédure pénale (*Federal Rules of Criminal Procedure*).

privée. C'est notamment le cas des Lignes directrices du procureur général pour les opérations nationales du Bureau d'enquête fédéral[18] qui exigent notamment que le Bureau d'enquête fédéral emploie les méthodes d'enquête les moins intrusives possibles en tenant compte de l'atteinte à vie privée et de la potentielle atteinte à la réputation.

Des garanties similaires s'appliquent aux enquêtes menées en vertu des législations des Etats. Les autorités chargées de l'application du droit pénal dans les Etats utilisent les mandats et les citations à comparaître essentiellement de la même manière que celle décrite pour les autorités fédérales, mais avec parfois des garanties supplémentaires prévues par les constitutions ou les législations des Etats. En tout état de cause, les garanties prévues au niveau des Etats doivent être au moins égales à celles de la Constitution des Etats-Unis.

Par ailleurs, des garanties similaires s'appliquent aux citations à comparaître administratives émises pour obtenir l'accès aux données détenues par les entreprises aux Etats-Unis à des fins civiles ou réglementaires, c'est-à-dire d'intérêt public. Les autorités ayant des responsabilités civiles et réglementaires ne peuvent demander l'accès qu'aux données qui sont pertinentes pour les questions relevant de leur pouvoir de réglementation[19]. En outre, le destinataire d'une citation à comparaître administrative peut en contester l'exécution devant un tribunal car la citation doit être raisonnable[20]. Bien que l'utilisation d'une citation administrative ne soit pas soumise à une approbation judiciaire préalable, elle devient soumise à un contrôle judiciaire en cas de contestation par le destinataire ou si l'autorité qui a émis la citation souhaite la faire appliquer devant un tribunal. Outre ces garanties générales, des exigences spécifiques plus strictes peuvent découler de certaines lois[21]. En tout état de cause, les exigences du quatrième amendement de la Constitution des Etats-Unis doivent être satisfaites.

A noter que les Etats-Unis, par l'intermédiaire du Département de la justice (DoJ), ont également confirmé les garanties applicables et limites à l'accès décrites ci-dessus par le biais d'un courrier[22].

---

[18] Ces lignes directrices sont accessibles sous le lien suivant : The Attorney General's Guidelines for Domestic FBI Operations (justice.gov).

[19] A cet égard, la jurisprudence de la Cour suprême des Etats-Unis a également précisé la nécessité de trouver un équilibre entre l'importance de l'intérêt public et l'importance des intérêts des personnes concernées en matière de protection de la vie privée. C.f. *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), accessible sous le lien suivant : U.S. Reports: Okla. Press Pub. Co. v. Walling, 327 U.S. 186 (1946). (loc.gov).

[20] C.f. critères mentionnés plus haut en relation avec les citations à comparaître dans le cadre d'enquêtes pénales.

[21] A titre d'exemple, les institutions financières peuvent contester les citations à comparaître administratives visant à obtenir certains types d'informations en invoquant la loi sur le secret bancaire et ses règlements d'application, c.f. notamment titre 31 du Code des Etats-Unis, réglementation relative à l'argent et aux finances, accessible sous le lien suivant : OLRC Home (house.gov).

[22] C.f. lettre du DoJ, accessible au moyen des liens vers les textes de référence en fin de document.

L'utilisation ultérieure des données collectées est régie par une politique centrale (circulaire n° A-130 du Bureau de Gestion et du Budget (*Office of Management and Budget, OMB*)[23] qui doit être mise en œuvre et respectée par toutes les autorités fédérales, y compris les autorités chargées de l'application de la loi, lorsqu'elles traitent des données personnelles identifiables. Les autorités sont tenues de limiter la création, la collecte, l'utilisation, le traitement, le stockage, la maintenance, la diffusion et la divulgation des données personnelles identifiables à celles qui sont légalement autorisées, pertinentes et raisonnablement jugées nécessaires à la bonne exécution des fonctions autorisées des autorités. Les autorités doivent mettre en place un programme complet de protection de la vie privée (p.ex. gérer les risques, détecter, documenter et signaler les incidents, etc.).

En vertu de la règlementation sur le gouvernement électronique[24], les autorités fédérales sont tenues de mettre en place des mesures de protection de la sécurité des données qui tiennent compte du risque et de l'importance du préjudice qui résulterait de l'accès, l'utilisation, la divulgation, l'interruption, la modification ou la destruction non autorisés des données. Elles doivent également nommer un directeur de l'information (*Chief Information Officer*) afin d'assurer le respect des exigences de sécurité des données et effectuer une évaluation indépendante chaque année. Des analyses des incidences sur la vie privée sont requises pour toutes les autorités fédérales qui développent ou acquièrent de nouvelles technologies de l'information qui collectent, conservent ou diffusent des données sous une forme identifiable ou qui mettent en place une nouvelle collecte de données.

L'OMB et l'institut national de normalisation et de technologie (*National Institute of Standards and Technology*) ont élaboré des normes qui sont contraignantes pour les agences fédérales (y compris les autorités chargées de l'application du droit pénal) et qui précisent les exigences minimales à mettre en place en matière de sécurité des données, notamment les contrôles d'accès, la sensibilisation et la formation, les plans d'urgence, la réponse aux incidents, les outils d'audit et de responsabilité, la garantie de l'intégrité des systèmes et des données, l'évaluation des risques en matière de sécurité et de protection de la vie privée, etc.[25]

La réglementation sur les documents fédéraux[26] stipule que les données détenues par les autorités fédérales doivent être soumises à des mesures de protection garantissant l'intégrité physique des données et la prévention d'un accès non autorisé.

En ce qui concerne la conservation des données, les autorités fédérales sont tenues d'établir des délais de conservation qui doivent être approuvées par les Archives nationales (*National*

---

[23] Accessible sous le lien suivant: Review-Doc-2016--466-1.docx (archives.gov).

[24] C.f. titre 44 chapitre 36 du Code des Etats-Unis.

[25] C.f. circulaire n° A-130 de l'OMB; NIST SP 800-53, Rev. 5, Control Mappings to ISO/IEC 27001, juillet 2023, accessible sous le lien suivant: SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov).

[26] C.f. titre 44 chapitre 31 du Code des Etats-Unis.

*Archives and Record Administration*)[27]. La durée du délai de conservation est fixée en fonction de différents facteurs tels que le type d'enquête ou la pertinence des éléments de preuve pour l'enquête.

### 4.1.2 Autorité indépendante, voies de droit

#### 4.1.2.1 Surveillance

Les activités des autorités fédérales d'application du droit pénal sont soumises au contrôle de divers organes[28]. Comme indiqué sous chiffre 4.1.1., il s'agit dans de nombreux cas de figure d'un contrôle préalable par le pouvoir judiciaire, qui doit autoriser les différentes mesures de collecte de données. En outre, d'autres organes supervisent les activités des autorités d'application du droit pénal. Ces organes judiciaires et non judiciaires garantissent un contrôle indépendant.

Tout d'abord, des délégués à la protection des libertés civiles et de la vie privée (*Civil Liberties and Privacy Officers, CLPO*, ci-après délégués) sont en place au sein de diverses autorités ayant des responsabilités en matière d'application du droit pénal[29]. Leurs attributions comprennent généralement la surveillance des procédures visant à garantir que l'autorité concernée prend en compte de manière appropriée les préoccupations en matière de de libertés civiles et de vie privée et a mis en place des procédures appropriées pour traiter les plaintes pour violation de la vie privée ou des libertés civiles. Les responsables de chaque autorité doivent veiller à ce que les délégués disposent des documents et des ressources nécessaires, qu'ils aient accès au matériel et au personnel nécessaires à l'exercice de leurs fonctions, et qu'ils soient informés et consultés sur les changements de politique proposés. Les délégués doivent régulièrement faire rapport au Congrès, notamment s'agissant du nombre de plaintes reçues par les autorités concernées, de leur nature et de la suite donnée ainsi que de l'impact des activités menées en tant que délégués.

Par ailleurs, un inspecteur général[30] indépendant[31] contrôle les activités du DoJ, y compris celles du Bureau fédéral d'enquête. L'inspecteur général est chargé de mener des enquêtes,

---

[27] C.f. titre 44 chapitre 29 du Code des Etats-Unis.

[28] Les mécanismes mentionnés sous chiffre 4.1.2.1. s'appliquent également à la collecte et à l'utilisation de données par les autorités fédérales à des fins civiles et réglementaires. Les autorités civiles et réglementaires fédérales sont soumises au contrôle de leurs inspecteurs généraux respectifs et au contrôle du Congrès.

[29] C.f. titre 42 chapitre 21E du Code des Etats-Unis.

[30] C.f. titre 5, partie I, chapitre 4 du Code des Etats-Unis.

[31] Les inspecteurs généraux sont inamovibles et ne peuvent être révoqués que par le président des Etats-Unis, qui doit communiquer par écrit au Congrès les raisons de cette révocation.

des audits et des inspections sur les programmes et les activités du DoJ de manière indépendante[32]. Il a accès à tous les dossiers, rapports, audits, examens, documents, recommandations ou autres éléments pertinents, si nécessaire sur citation, et peut recueillir des témoignages. Si l'inspecteur général formule des recommandations non contraignantes en vue de mesures correctives, ses rapports sont généralement rendus publics et transmis au Congrès, qui peut ainsi exercer sa fonction de contrôle. L'inspecteur général accepte et examine les plaintes déposées par des particuliers.

De plus, les autorités ayant des responsabilités en matière d'application du droit pénal sont soumises au contrôle du conseil de surveillance de la vie privée et des libertés civiles (*Privacy and Civil Liberties Oversight Board, PCLOB*, ci-après conseil de surveillance) dans la mesure où elles mènent des activités de lutte contre le terrorisme. Le conseil de surveillance est un organe indépendant au sein du pouvoir exécutif composée d'un conseil de cinq membres nommés par le président des Etats-Unis pour un mandat fixe de six ans avec l'approbation du Sénat ; il ne peut en aucun cas compter plus de trois membres appartenant au même parti politique[33]. Le conseil de surveillance a des responsabilités dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre, en vue de protéger la vie privée et les libertés civiles. Il peut accéder à tous les dossiers, rapports, audits, examens, documents et recommandations pertinents des autorités fédérales, y compris les informations classifiées, et peut recueillir des témoignages. Il reçoit des rapports des délégués de plusieurs autorités fédérales, peut émettre des recommandations aux autorités gouvernementales et aux autorités chargées de l'application de la loi, et fait régulièrement rapport aux commissions du Congrès et au président. Les rapports doivent être rendus publics dans toute la mesure du possible.

Enfin, les activités d'application du droit pénal sont soumises au contrôle de commissions spécifiques du Congrès (les commissions judiciaires de la Chambre et du Sénat). Ces commissions judiciaires exercent un contrôle régulier de différentes manières, notamment par le biais d'auditions, d'enquêtes, d'examens et de rapports.

#### 4.1.2.2 Voies de droit

Les autorités chargées de l'application du droit pénal doivent, dans la plupart des cas, obtenir une autorisation judiciaire préalable pour collecter des données personnelles. Cela n'est pas le cas pour les citations à comparaître administratives, mais celles-ci sont limitées à des situations spécifiques et font l'objet d'un contrôle judiciaire indépendant, du moins lorsque leur exécution est demandée par la voie judiciaire. En particulier, les destinataires de citations administratives peuvent les contester devant un tribunal au motif qu'elles ne sont pas raisonnables, c'est-à-dire qu'elles sont excessives, oppressives ou contraignantes. Les personnes concernées peuvent introduire des demandes ou des plaintes concernant le traitement de leurs données personnelles auprès des autorités chargées de l'application du droit pénal. Par ce biais, elles peuvent notamment demander l'accès à leurs données personnelles et leur

---

[32] C.f. plan stratégique 2020-2024 de l'inspecteur général du DoJ, accessible sous le lien suivant : Strategic Plan Draft - To AIGs (justice.gov).

[33] C.f. titre 42 chapitre 21E du Code des Etats-Unis.

rectification[34]. En ce qui concerne les activités liées à la lutte contre le terrorisme, les personnes concernées peuvent également déposer une plainte auprès des délégués au sein des autorités chargées de l'application du droit pénal[35].

En outre, plusieurs voies de recours judiciaires peuvent être utilisées à l'encontre d'une autorité ou de l'un de ses fonctionnaires, lorsque des données personnelles sont traitées. Ces voies de recours[36] sont ouvertes à toutes les personnes quelle que soit leur nationalité, sous réserve des conditions applicables.

De manière générale, en vertu des dispositions relatives au contrôle juridictionnel contenues dans la réglementation relative à la procédure administrative[37], toute personne subissant un dommage du fait d'une décision d'une autorité, ou affectée ou lésée par une telle décision, peut former un recours juridictionnel. Cela inclut la possibilité de demander au tribunal de déclarer illégale et d'annuler la décision, les constatations et les conclusions d'une autorité considérées comme arbitraires, futiles, constitutives d'un abus du pouvoir d'appréciation ou autrement non conformes au droit.

Par ailleurs et plus spécifiquement, la réglementation relative à la confidentialité des communications électroniques[38] établit un système de droits légaux à la vie privée et régit l'accès à des fins d'application de la loi au contenu des communications téléphoniques, orales ou électroniques stockées par des fournisseurs de services tiers. L'accès illicite, qui n'a pas été autorisé par un tribunal ou par ailleurs permis, est punissable ; les personnes concernées peuvent intenter une action au civil devant un tribunal fédéral américain pour demander des dommages-intérêts, y compris punitifs, ainsi qu'une réparation équitable ou une décision déclaratoire à l'encontre d'un fonctionnaire qui a délibérément commis de tels actes illégaux, ou à l'encontre des États-Unis.

Ensuite, plusieurs autres réglementations[39] confèrent aux personnes concernées le droit d'intenter une action contre une autorité ou un fonctionnaire américain en ce qui concerne le traitement de leurs données personnelles.

---

[34] C.f. circulaire n° A-130 de l'OMB.

[35] C.f. titre 42 chapitre 21E du Code des Etats-Unis.

[36] Voir notamment les réglementations relatives à la procédure administrative et à la transparence (c.f. titre 5 du Code des Etats-Unis) ainsi que la réglementation relative à la confidentialité des communications électroniques (c.f. titre 18 du Code des Etats-Unis).

[37] C.f. titre 5 du Code des Etats-Unis.

[38] C.f. titre 18, partie I, chapitre 121 du Code des Etats-Unis.

[39] C'est le cas notamment des réglementations relatives aux écoutes téléphoniques et à la fraude et aux abus informatiques (c.f. titre 18 du Code des Etats-Unis).

Enfin, en vertu de la réglementation relative à la transparence[40], toute personne a le droit d'obtenir l'accès à des informations d'autorités fédérales, y compris lorsque celles-ci contiennent des données personnelles. Après avoir épuisé les voies de recours administratives, une personne peut invoquer ce droit d'accès devant un tribunal, à moins que ces informations ne soient protégées de la divulgation publique par une dérogation ou une exclusion spéciale relative à l'application de la loi. Dans ce cas, le tribunal déterminera si une dérogation s'applique ou a été légalement invoquée par l'autorité concernée.

## 4.2 Accès à des fins de sécurité nationale

### 4.2.1 Législation applicable, garanties effectives

La collecte par les autorités des Etats-Unis à des fins de sécurité nationale de données personnelles transférées depuis la Suisse vers des organisations certifiées est assortie de conditions et garanties spécifiques. Il convient d'examiner en particulier les éléments liés à la collecte de renseignements d'origine électromagnétique (*signals intelligence*) qui a trait à la collecte de communications électroniques et de données provenant de systèmes d'information pouvant contenir des données personnelles.

Conformément au décret exécutif (*executive order*) 12333 de 1981[41] relatif aux activités des services de renseignement des Etats-Unis, des données personnelles peuvent être collectées en dehors des Etats-Unis et donc également lorsque de telles données sont en train d'être transférées de Suisse vers les Etats-Unis.

Par ailleurs, une fois que des données personnelles ont été reçues par des organisations certifiées aux Etats-Unis, les services de renseignement peuvent demander l'accès à ces données si la réglementation en vigueur l'autorise. De telles collectes de données peuvent notamment être autorisées par la réglementation sur la surveillance des renseignements étrangers (FISA)[42].

Le 7 octobre 2022, le président des Etats-Unis a publié le décret exécutif 14086[43] relatif au renforcement des garanties concernant les activités de renseignement d'origine électromagnétique ; ce décret remplace en grande partie[44] la directive présidentielle 28 (*Presidential Policy Directive 28, PPD-28*)[45]. Ce décret s'applique à toutes les activités de renseignement

---

40 C.f. titre 5 du Code des Etats-Unis.

41 C.f. Executive Orders | National Archives.

42 C.f. titre 50 chapitre 36 du Code des Etats-Unis.

43 C.f. liens vers les textes de référence en fin de document.

44 Le décret exécutif 14086 remplace la PPD-28 sauf en ce qui concerne certains articles spécifiques (révocation partielle de la PPD-28).

45 C.f. Presidential Policy Directive -- Signals Intelligence Activities | whitehouse.gov (archives.gov).

d'origine électromagnétique, soit il couvre tant les activités basées sur la FISA que celles basées sur le décret exécutif 12333 ; ses dispositions sont contraignantes pour l'ensemble de la communauté du renseignement des Etats-Unis. Il fixe des limites et garanties qui complètent celles prévues par la FISA et le décret exécutif 12333 et établit par ailleurs un nouveau mécanisme de recours permettant d'invoquer ces garanties et de les faire appliquer. Les agences du renseignement ont actualisé leurs politiques et procédures afin de les mettre en conformité avec les dispositions du décret exécutif 14086 ; après un processus comprenant diverses consultations notamment du procureur général, du CLPO de l'ODNI et du PCLOB, ces politiques et procédures ont été publiées le 3 juillet 2023[46].

Le décret exécutif 14086 fixe un catalogue d'exigences s'appliquant à toutes les activités de renseignement d'origine électromagnétique. Ces activités doivent être fondées sur une réglementation ou une autorisation présidentielle et doivent être effectuées en conformité avec la législation des Etats-Unis, notamment la Constitution. Des garanties appropriées doivent être mises en place pour tenir compte de la protection de la vie privée et des libertés civiles de tous les individus, indépendamment de leur nationalité ou de leur lieu de résidence, lors de la planification des activités. En particulier il convient d'avoir déterminé que, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, les activités sont nécessaires pour faire progresser une priorité validée en matière de renseignement. De plus, ces activités doivent être menées de manière proportionnée à une priorité validée en matière de renseignement pour laquelle elles ont été autorisées. Soit une pesée d'intérêt doit être effectuée entre l'importance de l'activité pour la priorité validée et l'incidence sur la vie privée et les libertés civiles de la personne concernée.

Les exigences susmentionnées sont renforcées par des garanties visant à ce que l'ingérence dans les droits des personnes concernées soit limitée à ce qui est nécessaire et proportionné pour atteindre un objectif légitime.

Tout d'abord, le décret limite les motifs pour lesquels des données peuvent être collectées dans le cadre d'activités de renseignement d'origine électromagnétique. D'une part, le décret définit les objectifs légitimes qui peuvent être poursuivis, par exemple comprendre ou évaluer les capacités, les intentions ou les activités d'organisations étrangères, notamment d'organisations terroristes internationales, qui constituent une menace actuelle ou potentielle pour la sécurité nationale des États-Unis. D'autre part, le décret énumère certains objectifs qui ne doivent jamais être poursuivis, par exemple dans le but d'entraver la libre expression d'idées ou d'opinions politiques par des personnes ou par la presse. De plus, la collecte effective ne peut avoir lieu que pour faire progresser une priorité en matière de renseignement ; or les priorités sont établies par la directrice du renseignement national et font l'objet d'une évaluation par le CLPO de l'ODNI, elles sont ensuite soumises à l'approbation du président des Etats-Unis. Cette procédure garantit que les aspects relatifs à la protection de la vie privée sont pris en compte dans le cadre de l'élaboration des priorités en matière de renseignement.

Ensuite, une fois qu'une priorité en matière de renseignement a été établie, des exigences régissent la décision de savoir si et dans quelle mesure des renseignements d'origine électro-

[46] C.f. INTEL - ODNI Releases IC Procedures Implementing New Safeguards in Executive Order 14086.

magnétique peuvent être collectés pour faire avancer cette priorité. Ces exigences concrétisent les normes générales de nécessité et de proportionnalité énoncées dans le décret. Ainsi les renseignements d'origine électromagnétique ne peuvent être collectés qu'après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, que la collecte est nécessaire pour faire progresser une priorité spécifique en matière de renseignement. Pour déterminer cet élément de nécessité, les agences de renseignement doivent examiner la disponibilité, la faisabilité et la validité d'autres sources et méthodes moins intrusives et, lorsqu'elles sont disponibles, la priorité doit être donnée à ces autres sources et méthodes moins intrusives.

Lorsque la collecte est jugée nécessaire, elle doit être aussi ciblée que possible. Afin de prévenir un effet disproportionné sur la vie privée et les libertés civiles, c'est-à-dire de trouver un juste équilibre entre les besoins de sécurité nationale et la protection de la vie privée et des libertés civiles, tous les facteurs pertinents doivent être dûment pris en compte, tels que la nature de l'objectif poursuivi; le caractère intrusif de la collecte, notamment sa durée; la contribution probable de la collecte à l'objectif poursuivi; les conséquences raisonnablement prévisibles pour les personnes concernées; et la nature et le caractère sensible des données à collecter.

La collecte en vrac de renseignements d'origine électromagnétique, c'est-à-dire la collecte de grandes quantités de renseignements d'origine électromagnétique qui est effectuée sans utiliser par exemple des critères de sélection spécifiques[47], ne peut avoir lieu qu'en dehors des Etats-Unis, sur la base du décret exécutif 12333. Cependant la priorité doit être donnée à une collecte ciblée. Conformément au décret exécutif 14086, la collecte en vrac n'est autorisée que lorsque les informations nécessaires pour faire progresser une priorité validée en matière de renseignement ne peuvent raisonnablement pas être obtenues par une collecte ciblée et des garanties spécifiques s'appliquent: des méthodes et des mesures techniques doivent être appliquées afin de limiter les données collectées à ce qui est nécessaire pour faire progresser une priorité validée en matière de renseignement, tout en réduisant autant que possible la collecte d'informations non pertinentes; l'utilisation des informations collectées en vrac est limitée à six objectifs définis, notamment la protection contre le terrorisme et la protection contre l'espionnage étranger, le sabotage ou l'assassinat. Enfin, toute interrogation de données de renseignement d'origine électromagnétique obtenues en vrac ne peut avoir lieu que si elle est nécessaire pour faire progresser une priorité validée en matière de renseignement, dans le cadre de la poursuite de ces six objectifs et conformément à des politiques et procédures qui tiennent dûment compte de l'incidence des interrogations de données sur la vie privée et les libertés civiles de toutes les personnes, quels que soient leur nationalité ou leur lieu de résidence.

Outre les exigences du décret exécutif 14086, la collecte de données de renseignement d'origine électromagnétique transférées vers une organisation certifiée aux Etats-Unis est soumise à des limitations et garanties spécifiques régies par l'article 702 de la FISA, selon lequel le procureur général et la directrice du renseignement national soumettent des certifications annuelles au tribunal de la surveillance du renseignement étranger (*Foreign Intelligence Sur-*

[47] La collecte en vrac se distingue toutefois de la collecte généralisée et indifférenciée (« surveillance de masse ») sans restrictions ni garanties.

*veillance Court, FISC*) qui déterminent des catégories de renseignements étrangers à collecter. Les certifications doivent être accompagnées de procédures de ciblage, de minimisation et d'interrogation, qui sont également approuvées par le tribunal et sont juridiquement contraignantes pour les agences de renseignement.

Le FISC est un tribunal indépendant dont les décisions peuvent être contestées devant la cour révisant les décisions en matière de surveillance du renseignement extérieur et, en dernier recours, devant la Cour suprême des Etats-Unis[48]. Le FISC reçoit l'appui d'un panel permanent de cinq avocats et cinq experts techniques qui ont une expertise en matière de sécurité nationale et de libertés civiles, garantissant ainsi que les questions de protection de la vie privée sont dûment prises en compte.

Les décisions de ciblage individuel sont prises par l'agence nationale de sécurité (*National Security Agency, NSA*) conformément aux procédures de ciblage approuvées par le FISC, qui exigent que la NSA évalue, sur la base de l'ensemble des circonstances, que le ciblage d'une personne donnée est susceptible de permettre l'obtention d'une catégorie de renseignements étrangers indiquée dans une certification. Le ciblage est effectué en choisissant des sélecteurs qui recensent des moyens de communication spécifiques, comme l'adresse électronique ou le numéro de téléphone d'une cible, et non pas des mots clés ou les noms des personnes ciblées. La NSA doit documenter la base factuelle de la sélection de la cible et, à intervalles réguliers après le ciblage initial, confirmer que la norme de ciblage continue d'être respectée, sans quoi la collecte doit cesser. La sélection de chaque cible par la NSA et l'enregistrement de chaque évaluation et justification de ciblage sont vérifiés tous les deux mois par les bureaux de surveillance du renseignement du DoJ, qui sont tenus de signaler toute violation au FISC et au Congrès.

En ce qui concerne les autres bases légales permettant de collecter des données personnelles transférées vers des organisations certifiées aux États-Unis, différentes restrictions et garanties s'appliquent. En général, la collecte de données en vrac est spécifiquement interdite et l'utilisation de critères de sélection spécifiques est requise. Pour procéder à une surveillance électronique des individus, les agences de renseignement doivent soumettre une demande au FISC, accompagnée d'un exposé des faits et circonstances invoqués à l'appui de la conviction qu'il existe un motif sérieux de croire que l'installation est utilisée ou sur le point d'être utilisée par une puissance étrangère ou un agent d'une puissance étrangère. Le FISC appréciera, entre autres, si sur la base des faits soumis, il existe une présomption sérieuse que cela est le cas. Une demande doit également être soumise au FISC pour effectuer une perquisition dans des locaux ou sur des biens qui doit aboutir à une inspection ou une saisie d'informations, de matériel ou de biens ou pour l'installation de dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications.

Le traitement des données personnelles collectées par les agences de renseignement américaines au moyen de renseignements d'origine électromagnétique fait par ailleurs l'objet de garanties. Tout d'abord, chaque agence de renseignement doit garantir une sécurité appropriée des données et empêcher l'accès des personnes non autorisées aux données person-

[48] C.f. titre 50 chapitre 36 du Code des Etats-Unis.

nelles collectées au moyen de renseignements d'origine électromagnétique. L'accès aux données collectées doit être limité au personnel autorisé et formé qui a besoin de connaître ces informations pour mener à bien sa mission. Plus généralement, les agences de renseignement doivent proposer une formation appropriée à leurs employés. Par ailleurs, les agences de renseignement doivent se conformer aux normes de la communauté du renseignement en matière d'exactitude et d'objectivité, notamment en ce qui concerne la qualité et la fiabilité des données, la prise en compte d'autres sources d'information et l'objectivité dans la réalisation des analyses. De plus, en ce qui concerne la conservation des données, les durées de conservations s'appliquent indépendamment de la nationalité des personnes concernées. Ensuite, des règles spécifiques s'appliquent à la diffusion des données personnelles collectées au moyen de renseignements d'origine électromagnétique. A titre d'exemple, les données personnelles ne peuvent être diffusées uniquement en raison de la nationalité ou du pays de résidence d'une personne ou dans le but de contourner les exigences du décret exécutif 14086. Enfin, afin de faciliter le contrôle du respect des exigences légales applicables et d'offrir des voies de recours efficaces, chaque agence de renseignement est tenue de conserver une documentation appropriée sur la collecte de renseignements d'origine électromagnétique. Outre les garanties susmentionnées du décret exécutif 14086 en ce qui concerne l'utilisation des données collectées au moyen de renseignements d'origine électromagnétique, les agences de renseignement sont soumises à des exigences plus générales en matière de limitation des finalités, de minimisation des données, d'exactitude, de sécurité, de conservation et de diffusion, découlant notamment de l'instruction 1253 du Comité des systèmes de sécurité nationale (CNSSi) relative à la catégorisation de la sécurité et à la sélection des contrôles pour les systèmes de sécurité nationale, de la circulaire n° A-130 de l' Office de gestion et du budget (OMB) et d'autres réglementations applicables.

### 4.2.2 Autorité indépendante, voies de droit

#### 4.2.2.1 Surveillance

Les activités des agences de renseignement font l'objet d'une surveillance de la part de différents organismes. Tout d'abord, le décret exécutif 14086 exige que chaque agence de renseignement dispose de responsables juridiques et de délégués chargés de la surveillance et du respect des règles de haut niveau afin de garantir le respect du droit national applicable. En particulier, ils doivent surveiller régulièrement les activités de renseignement d'origine électromagnétique et veiller à ce que tout cas de non-respect soit corrigé. Les agences de renseignement doivent donner à ces responsables l'accès à toutes les informations pertinentes pour l'exercice de leurs fonctions et ne peuvent prendre aucune mesure pour entraver ou influencer indûment leurs activités de surveillance. En outre, tout cas de non-respect significatif constaté par un délégué chargé de la surveillance ou toute autre personne doit être rapidement signalé au chef de l'agence de renseignement et à la directrice du renseignement national, qui doivent veiller à ce que toutes les mesures nécessaires soient prises pour corriger ce cas et empêcher qu'il ne se reproduise.

Comme c'est le cas en ce qui concerne les autorités d'application du droit pénal, des CLPOs sont en place dans toutes les agences de renseignement[49]. Les pouvoirs des CLPOs englobent généralement la surveillance des procédures permettant de veiller à ce que le service

[49] C.f. titre 42 du Code des Etats-Unis.

concerné/l'agence concernée prenne en compte de façon adéquate les problèmes touchant à la vie privée et aux libertés civiles et ait mis en place des procédures appropriées pour traiter les réclamations émanant de personnes qui estiment que leur vie privée ou les libertés civiles ont été violées. Les chefs de service ou de l'agence doivent veiller à ce que les CLPOs disposent des ressources nécessaires à l'accomplissement de leur mandat, se voient accorder l'accès à tous les documents et au personnel nécessaires pour pouvoir s'acquitter de leurs fonctions et soient informés et consultés sur les changements de politique proposés. Les CLPOs font régulièrement rapport au Congrès et au PCLOB, notamment sur le nombre et la nature des réclamations par le service/l'agence, les informent succinctement du sort réservé à ces réclamations, et les renseignent sur les examens et les enquêtes effectués ainsi que sur l'impact des activités menées.

Par ailleurs, chaque agence de renseignement compte un inspecteur général indépendant chargé, entre autres, de contrôler les activités de renseignement extérieur. Ainsi, au sein de l'ODNI, le bureau de l'inspecteur général de la communauté du renseignement est doté de vastes attributions en ce qui concerne l'ensemble des services de renseignement. Ces inspecteurs généraux sont indépendants et sont chargés d'effectuer des audits et des enquêtes sur les activités et programmes menés par l'agence concernée à des fins de renseignement national, y compris en ce qui concerne des abus ou une violation du droit. Ils ont accès à l'ensemble des archives, rapports, audits, réexamens, documents, recommandations ou à tout autre matériel pertinent, si nécessaire au moyen d'une citation, et ils peuvent recueillir des témoignages. Les inspecteurs généraux signalent les cas d'infractions pénales présumées à des fins de poursuites et formulent des recommandations sur l'adoption de mesures correctives à l'intention des chefs d'agence. Si leurs recommandations sont non contraignantes, leurs rapports, notamment sur les mesures de suivi (ou leur absence) sont généralement rendus publics et transmis au Congrès qui peut, sur cette base, exercer sa propre fonction de contrôle.

Ensuite, le conseil de surveillance du renseignement (*Intelligence Oversight Board, IOB*), qui est établi au sein du conseil consultatif en matière de renseignement relevant du président des Etats-Unis (*President's Intelligence Advisory Board, PIAB*), supervise le respect de la Constitution et des autres réglementations applicables par les autorités de renseignement. Le PIAB est composé de 16 membres nommés par le président et ne faisant pas partie du gouvernement des Etats-Unis. L'IOB est composé d'un maximum de cinq membres désignés par le président parmi les membres du PIAB. En vertu du décret exécutif 12333, les chefs de toutes les agences de renseignement sont tenus de signaler à l'IOB toute activité de renseignement dont ils ont des raisons de croire qu'elle pourrait être illégale ou contraire à un décret ou à une directive présidentielle. L'IOB est à son tour tenu d'informer le président des activités de renseignement dont il estime qu'elles peuvent constituer une violation du droit national (notamment des décrets) et qu'elles ne sont pas traitées de manière appropriée par le procureur général, la directrice du renseignement national ou le chef d'une agence de renseignement. En outre, l'IOB est tenu d'informer le procureur général d'éventuelles violations du droit pénal.

De plus, les agences de renseignement sont soumises au contrôle du PCLOB. Selon son statut fondateur, le PCLOB est investi de responsabilités dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre en vue de protéger la vie privée et les libertés civiles. Dans le cadre de son examen des activités des agences de renseignement, il peut accéder à l'ensemble des archives, rapports, audits, analyses, documents, pièces et recommandations pertinents, notamment aux informations classifiées et recueillir des témoignages.

Il peut adresser des recommandations aux autorités et fait régulièrement rapport aux commissions du Congrès et au président. Les rapports du PCLOB, y compris ceux destinés au Congrès, doivent être rendus publics dans la mesure la plus large possible. Le PCLOB est également chargé d'exercer des fonctions de surveillance spécifiques en ce qui concerne la mise en œuvre du décret exécutif 14086, notamment en vérifiant si les procédures des agences sont conformes au décret et en évaluant le fonctionnement correct du mécanisme de recours (c.f. ch. 4.2.2.2).

Outre ces mécanismes de contrôle au sein du pouvoir exécutif, des commissions spéciales au sein du Congrès (les commissions du renseignement et judiciaires de la Chambre des représentants et du Sénat) exercent des responsabilités de surveillance à l'égard de toutes les activités du renseignement extérieur. Les membres de ces commissions ont accès à des informations classifiées et aux méthodes et programmes de renseignement. Les commissions exercent leurs fonctions de surveillance de différentes manières, notamment au moyen d'auditions, d'enquêtes, d'examens et de rapports. Les commissions du Congrès reçoivent des rapports réguliers sur les activités de renseignement, notamment de la part du procureur général, de la directrice du renseignement national, des agences de renseignement et d'autres organes de surveillance (par exemple, les inspecteurs généraux).

Plus généralement, la communauté du renseignement des États-Unis entreprend divers efforts pour assurer la transparence de ses activités de renseignement. En 2015, par exemple, l'ODNI a adopté des principes de transparence en matière de renseignement et un plan de mise en œuvre de la transparence[50]. Dans ce contexte, la communauté du renseignement a rendu et continue de rendre publiques des parties déclassifiées de politiques, de procédures, de rapports de surveillance, etc.

Enfin, la collecte de données personnelles en vertu de la FISA fait l'objet également d'une surveillance de la part du FISC. Le cas échéant, le FISC peut ordonner à l'agence de renseignement compétente de prendre des mesures correctives. Les mesures en question peuvent être d'ordre individuel ou structurel, et aller, par exemple, de l'arrêt de l'acquisition de données à la suppression de données obtenues illégalement en passant par le changement de pratique en matière de collecte des données. En outre, lors de son examen annuel des certifications, le FISC examine les cas de non-respect afin de déterminer si les certifications soumises sont conformes aux exigences de la FISA. De même, si le FISC estime que les certifications demandées par le gouvernement au titre de l'article 702 de la FISA ne sont pas suffisantes, notamment en raison de cas de non-respect particuliers, il peut délivrer une ordonnance de manquement (*deficiency order*) exigeant du gouvernement qu'il remédie à la violation dans un délai de 30 jours ou qu'il cesse ou ne mette pas en œuvre la certification. Le FISC évalue les problèmes de conformité qu'il constate et peut exiger des changements de procédure ou une surveillance et des rapports supplémentaires pour résoudre ces problèmes.

#### 4.2.2.2 Voies de droit

Des voies de droit offrent la possibilité d'intenter une action en justice devant un tribunal indépendant et impartial. Ces voies de droit permettent aux personnes concernées d'avoir accès

[50] C.f. The Principles of Intelligence Transparency for the IC (dni.gov).

à leurs données personnelles, de faire contrôler la licéité de l'accès des autorités publiques à leurs données et, si une violation est constatée, d'y remédier, notamment par la rectification ou la suppression de leurs données personnelles.

En vertu du décret exécutif 14086, un mécanisme de recours spécifique est mis en place, complété par le règlement sur la cour d'examen en matière de protection des données (*Data Protection Review Court, DPRC*) du procureur général des États-Unis publié le 7 octobre 2022, afin de traiter et de résoudre les réclamations déposées par des personnes concernant les activités de renseignement d'origine électromagnétique des Etats-Unis. Toute personne concernée en Suisse a le droit d'introduire une plainte auprès du mécanisme de recours concernant une violation présumée du droit des Etats-Unis régissant les activités de renseignement d'origine électromagnétique qui porte atteinte à ses intérêts en matière de protection de la vie privée et de libertés civiles. Ce mécanisme de recours en matière de renseignements d'origine électromagnétique est accessible aux personnes originaires d'Etats ou d'organisations régionales d'intégration économique désignés par le procureur général des États-Unis. Le 7 juin 2024, la Suisse a été désignée en tant qu'Etat admissible pour le mécanisme de recours[51].

Une personne concernée en Suisse qui souhaite introduire une telle plainte doit la soumettre en premier lieu au PFPDT en tant qu'autorité indépendante de contrôle chargée de la protection des données en Suisse et l'autorité publique compétente pour transmettre les plaintes dans le cadre du mécanisme de recours. Ce procédé permet de garantir un accès simple au mécanisme de recours en permettant aux personnes concernées de s'adresser à une autorité avec laquelle elles peuvent communiquer dans leur langue. Afin de donner un point de départ au mécanisme de recours pour effectuer un examen, des informations doivent être fournies pour vérifier que la plainte concerne un individu et certaines informations de base doivent être fournies en ce qui concerne les données personnelles telles que adresse e-mail ou numéro de téléphone dont il est raisonnable de penser qu'elles ont été transférées vers les Etats-Unis et les moyens par lesquels on peut penser qu'elles ont été transférées, l'identité des entités du gouvernement des Etats-Unis soupçonnées d'être impliquées dans la violation présumée (pour autant que cette identité soit connue) et la nature de la réparation demandée, par exemple l'effacement des données concernées. En revanche, il n'est pas nécessaire de démontrer que les données personnelles ont effectivement été collectées par les agences de renseignement ou qu'elles ont fait l'objet d'activités de renseignement d'origine électromagnétique. Dans ce contexte, le PFPDT reçoit la plainte et vérifie simplement l'identité de la personne et contrôle si les informations de base ont bien été fournies. Si tel est le cas, le PFPDT transmet la plainte au mécanisme de recours.

L'enquête initiale sur les plaintes déposées auprès du mécanisme de recours est menée par le CLPO de l'ODNI, dont le rôle et les pouvoirs existants ont été étendus aux mesures spécifiques prises en vertu du décret exécutif 14086. Par ailleurs, la directive 126 de la communauté du renseignement[52] établie par le bureau de la directrice du renseignement national détaille les procédures de mise en œuvre pour le mécanisme de recours en matière de

[51] C.f. liens vers les textes de référence en fin de document.

[52] C.f. liens vers les textes de référence en fin de document.

renseignement selon le décret exécutif 14086. Au sein de la communauté du renseignement, le CLPO de l'ODNI est notamment chargé de veiller à ce que la protection des libertés civiles et de la vie privée soit intégrée de manière appropriée dans les politiques et procédures de l'ODNI et des agences de renseignement, de veiller à ce que l'ODNI respecte les exigences applicables en matière de protection de la vie privée et des libertés civiles et de procéder à des analyses des incidences sur la vie privée. Le CLPO de l'ODNI ne peut être démis de ses fonctions par la directrice du renseignement national que pour un juste motif, c'est-à-dire en cas de faute, de commission d'un délit, d'atteinte à la sécurité, de négligence ou d'incapacité. Lors de son examen, le CLPO de l'ODNI a accès aux informations nécessaires à son évaluation et peut compter sur l'assistance obligatoire des CLPOs des différentes agences de renseignement. Les agences de renseignement ont l'interdiction d'entraver ou d'influencer indûment les examens. Cela inclut la directrice du renseignement national, qui ne doit pas entraver l'examen. Lorsqu'il examine une plainte, le CLPO de l'ODNI doit appliquer la loi de manière impartiale, en tenant compte à la fois des intérêts de sécurité nationale concernant les activités de renseignement et de la protection de la vie privée. Dans le cadre de son examen, le CLPO de l'ODNI détermine s'il y a eu violation du droit des Etats-Unis applicable et, le cas échéant, décide d'une mesure corrective appropriée. Il s'agit de mesures visant à remédier pleinement à une violation constatée, telles que la cessation de l'obtention illicite de données, la suppression des données collectées illégalement, la suppression des résultats d'interrogations inappropriées de données par ailleurs collectées de manière légale, la limitation de l'accès à des données collectées de manière légale à du personnel dûment formé, ou le rappel des rapports de renseignement contenant des données acquises sans autorisation légale ou qui ont été diffusées de manière illégale. Les décisions du CLPO de l'ODNI sur les plaintes individuelles sont contraignantes pour les agences de renseignement concernées, y compris s'agissant des mesures correctives sauf si la DPRC, dont il est question ci-dessous, rend ultérieurement une décision contraire. Le CLPO de l'ODNI doit conserver la documentation relative à son examen et publier une décision classifiée expliquant le fondement de ses constatations factuelles, l'établissement de l'existence d'une violation couverte et le choix de la mesure corrective appropriée. Si l'examen révèle une violation commise par une autorité faisant l'objet d'une surveillance de la part du FISC, un rapport classifié doit également être fourni à l'assistant du procureur général chargé de la sécurité nationale, qui est à son tour tenu de signaler le non-respect au FISC, qui peut prendre d'autres mesures.

Une fois l'examen terminé, le CLPO de l'ODNI informe le plaignant au moyen d'une réponse standard, par l'intermédiaire du PFPDT, que l'examen n'a pas mis en évidence de violations couvertes ou qu'une décision exigeant des mesures correctives appropriées a été rendue. Cela permet de protéger la confidentialité des activités menées afin de protéger la sécurité nationale, tout en fournissant aux personnes concernées une décision confirmant que leur plainte a été dûment examinée et jugée. Cette décision peut d'ailleurs être contestée par la personne concernée. À cette fin, la personne concernée est informée de la possibilité de faire appel auprès de la DPRC pour un réexamen des décisions du CLPO de l'ODNI et du fait que, dans le cas où la personne concernée fait appel auprès de la DPRC, un avocat spécial sera sélectionné pour plaider en faveur des intérêts du plaignant dans l'affaire et veiller à ce que le panel de la DPRC soit bien informé des questions et de la loi relatives à l'affaire.

Tout plaignant, ainsi que chaque composante de la communauté du renseignement, peut faire appel afin de demander le réexamen de la décision du CLPO de l'ODNI devant la DPRC. Si une composante de la communauté du renseignement demande un examen auprès de la DPRC, un avocat spécial sera également désigné pour plaider en faveur des intérêts du plaignant dans l'affaire et veiller à ce que le panel de la DPRC soit bien informé des questions et de la loi relatives à l'affaire. Ces demandes de réexamen doivent être soumises

dans les 60 jours suivant la réception de la notification du CLPO de l'ODNI indiquant que son examen est terminé et inclure toute information que la personne concernée souhaite communiquer à la DPRC, tels que des arguments sur des questions de droit. Les personnes concernées de Suisse doivent soumettre leur demande de réexamen par l'intermédiaire du PFPDT qui transmettra ensuite la demande de réexamen de la personne concernée à la DPRC.

La DPRC est une cour indépendante établie par le procureur général sur la base du décret exécutif 14086. Elle est composée d'au moins six juges, nommés par le procureur général en consultation avec le PCLOB, le secrétaire d'Etat américain au commerce et la directrice du renseignement national pour des mandats renouvelables de quatre ans. La nomination des juges par le procureur général s'appuie sur les critères utilisés par le pouvoir exécutif pour évaluer les candidats à la magistrature fédérale, en tenant compte de leur expérience judiciaire antérieure. En outre, les juges doivent être des praticiens du droit (c'est-à-dire des membres actifs en règle du barreau et dûment autorisés à pratiquer le droit) et avoir une expérience appropriée en matière de droit de la protection de la vie privée et de la sécurité nationale. Le procureur général doit veiller à ce qu'au moins la moitié des juges aient une expérience judiciaire antérieure et tous les juges doivent être titulaires d'une habilitation de sécurité afin de pouvoir accéder à des informations classifiées relatives à la sécurité nationale. Par ailleurs, les juges ne doivent pas être employés du pouvoir exécutif au moment de leur nomination ou ne pas l'avoir été au cours des deux années précédentes. De même, pendant la durée de leur mandat à la DPRC, les juges ne peuvent exercer aucune fonction officielle ni aucun emploi au sein du gouvernement des Etats-Unis, autre que celui de juge à la DPRC. L'indépendance du processus de décision est assurée par plusieurs garanties. En particulier, il est interdit au pouvoir exécutif (le procureur général et les agences de renseignement) d'entraver ou d'influencer indûment l'examen de la DPRC. La DPRC elle-même est tenue de statuer de manière impartiale et fonctionne selon son propre règlement adopté à la majorité. En outre, les juges de la DPRC ne peuvent être révoqués que par le procureur général et qu'en cas de juste motif (faute, commission d'un délit, atteinte à la sécurité, négligence ou incapacité), après avoir dûment pris en compte les normes applicables aux juges fédéraux énoncées dans les règles relatives à la déontologie judiciaire et à la procédure d'incapacité judiciaire[53].

Les demandes adressées à la DPRC sont examinées par des panels de trois juges, dont un juge président, qui doivent agir conformément au code de conduite des juges aux Etats-Unis. Chaque panel est assisté d'un avocat spécial, qui a accès à toutes les informations relatives à l'affaire, y compris aux informations classifiées. Le rôle de cet avocat est de veiller à ce que les intérêts du plaignant soient représentés et à ce que le panel de juges de la DPRC soit bien informé de toutes les questions de droit et de fait pertinentes. Lorsque le plaignant a introduit une demande de réexamen, , l'avocat spécial peut demander des informations au plaignant en lui posant des questions écrites pour éclairer sa position sur une demande de réexamen introduite par un individu auprès de la DPRC. La DPRC examine les décisions prises par le CLPO de l'ODNI tant en ce qui concerne l'existence d'une violation du droit applicable des Etats-Unis qu'en ce qui concerne les mesures correctives appropriées, en se fondant, au minimum, sur le dossier de l'enquête du CLPO de l'ODNI, ainsi que sur les informations et

[53] C.f. décret exécutif 14086 et règlement du procureur général. Voir également le site Internet de la DPRC, qui présente la liste des juges actuels et leurs parcours: https://www.justice.gov/opcl/redress-data-protection-review-court.

observations fournies par le plaignant, l'avocat spécial ou une agence de renseignement. Un panel de juges de la DPRC a accès à toutes les informations nécessaires à la conduite d'un examen, qu'il peut obtenir par l'intermédiaire du CLPO de l'ODNI.

Au terme de son examen, la DPRC peut décider qu'il n'existe aucun élément de preuve indiquant que des activités de renseignement d'origine électromagnétique impliquant des données personnelles du plaignant ont eu lieu, ou décider que les décisions du CLPO de l'ODNI étaient juridiquement correctes et étayées par des preuves substantielles, ou rendre ses propres décisions si la DPRC est en désaccord avec les décisions du CLPO de l'ODNI. Lorsque la DPRC émet une décision qui diverge de celle du CLPO de l'ODNI, la décision de la DPRC prévaut et est contraignante pour le CLPO de l'ODNI et les agences de renseignement.

Dans tous les cas, la DPRC adopte une décision écrite à la majorité. Si l'examen révèle une violation des règles applicables, la décision précisera les mesures correctives appropriées, telles que la suppression des données collectées illégalement, la suppression des résultats d'interrogations inappropriées de données, la limitation de l'accès à des données collectées de manière légale à du personnel dûment formé, ou le rappel des rapports de renseignement contenant des données acquises sans autorisation légale ou qui ont été diffusées de manière illégale. La décision de la DPRC est contraignante et définitive en ce qui concerne la plainte dont elle est saisie. En outre, si l'examen révèle une violation commise par une autorité faisant l'objet d'une surveillance de la part du FISC, la DPRC doit également fournir un rapport classifié à l'assistant du procureur général chargé de la sécurité nationale, qui est à son tour tenu de signaler le non-respect au FISC, qui peut prendre d'autres mesures. Toute décision d'un panel de juges de la DPRC est transmise au CLPO de l'ODNI. Dans les cas où l'examen de la DPRC a été déclenché par une demande du plaignant, ce dernier est informé au moyen d'une réponse standard par l'intermédiaire du PFPDT que la DPRC a achevé son examen et que l'examen n'a pas mis en évidence de violations couvertes ou que la DPRC a rendu une décision exigeant des mesures correctives appropriées. Le bureau des libertés civiles et de la vie privée du DoJ conserve une archive de toutes les informations examinées par la DPRC et de toutes les décisions rendues, qui est mise à la disposition des futurs panels de juges de la DPRC en tant que précédent non contraignant. Le DoC est également tenu de conserver une archive pour chaque plaignant ayant déposé une plainte. Afin d'améliorer la transparence, le DoC doit, au moins tous les cinq ans, contacter les agences de renseignement concernées pour vérifier si les informations relatives à un examen par le CLPO de l'ODNI ou à un examen par la DPRC ont été déclassifiées. Si tel est le cas, la personne concernée sera informée par l'intermédiaire de l'autorité publique compétente que ces informations peuvent être disponibles en vertu du droit applicable.

Enfin, le bon fonctionnement de ce mécanisme de recours fera l'objet d'une évaluation régulière et indépendante. Plus précisément, le fonctionnement du mécanisme de recours est soumis à un examen annuel par le PCLOB, un organe indépendant[54]. Dans le cadre de cet examen, le PCLOB évalue notamment si le CLPO de l'ODNI et la DPRC ont traité les plaintes dans les délais impartis ; s'ils ont eu pleinement accès aux informations nécessaires ; si les

[54] Le décret exécutif 14086 encourage le PCLOB à procéder à un examen annuel du fonctionnement du mécanisme de recours. Le PCLOB a accepté de procéder à ces examens (voir Oversight Projects - PCLOB).

garanties substantielles du décret exécutif 14086 ont été correctement prises en compte dans la procédure d'examen ; et si la communauté du renseignement s'est pleinement conformée aux décisions. Le PCLOB présente un rapport sur les résultats de son examen au président des Etats-Unis, au procureur général, à la directrice du renseignement national, aux chefs des agences de renseignement, au CLPO de l'ODNI et aux commissions du renseignement du Congrès ; ce rapport sera également rendu public dans une version non classifiée. Le procureur général, la directrice du renseignement national, le CLPO de l'ODNI et les chefs des agences de renseignement sont tenus de mettre en œuvre toutes les recommandations figurant dans ces rapports ou d'y donner suite d'une autre manière. En outre, le PCLOB certifiera publiquement chaque année que le mécanisme de recours traite les réclamations conformément aux exigences du décret exécutif 14086.

Outre le mécanisme de recours spécifique établi par le décret exécutif 14086, des voies de recours devant les juridictions américaines ordinaires sont le cas échéant à la disposition des personnes concernées quelle que soit leur nationalité ou leur lieu de résidence. En particulier, la FISA et une loi connexe prévoient la possibilité pour les personnes concernées d'intenter un recours civil pour demander des dommages et intérêts aux Etats-Unis lorsque des informations à leur sujet ont été utilisées ou divulguées illégalement et volontairement, de poursuivre des fonctionnaires des Etats-Unis à titre personnel pour obtenir des dommages et intérêts et de contester la légalité de la surveillance dans le cas où le gouvernement envisagerait d'utiliser ou de divulguer toute information obtenue ou découlant de la surveillance électronique à l'encontre de la personne visée par une procédure judiciaire ou administrative aux Etats-Unis. Une possibilité plus générale de recours est contenue dans la réglementation relative à la procédure administrative, selon laquelle toute personne subissant un dommage du fait d'une décision d'une agence ou qui est affectée ou lésée par la décision d'une agence peut former un recours juridictionnel.

Enfin, en vertu de la réglementation relative à la transparence[55], toute personne a le droit d'obtenir l'accès à des informations d'autorités fédérales, y compris lorsque celles-ci contiennent des données personnelles. L'obtention de cet accès peut également faciliter l'introduction de procédures devant les juridictions ordinaires, notamment pour démontrer sa qualité à agir. Les agences peuvent ne pas divulguer les informations qui relèvent de certaines exceptions énumérées, notamment l'accès à des informations classifiées relatives à la sécurité nationale et à des informations concernant les enquêtes des autorités d'application du droit pénal, mais les plaignants qui ne sont pas satisfaits de la réponse ont la possibilité de la contester en demandant un contrôle administratif et, par la suite, un contrôle juridictionnel devant les juridictions fédérales.

## 5 Autres critères

### 5.1 Engagements internationaux

Il y a lieu de tenir compte des engagements internationaux. A cet égard, les engagements en matière de protection des données ne sont pas les seuls engagements pertinents et d'autres

[55] C.f. titre 5 du Code des Etats-Unis.

types d'engagements peuvent être pris en compte, par exemple les accords réglant l'échange d'informations.

Les Etats-Unis sont parties à certains cadres internationaux qui comportent des engagements en matière de droit à la vie privée et de droits humains en général.

En tant que membre de l'Organisation de coopération et de développement économiques (OCDE), les Etats-Unis participent aux travaux de l'OCDE sur la gouvernance des données et la protection de la vie privée. Ils se sont engagés à respecter le cadre de protection de la vie privée de l'OCDE, en particulier les Lignes directrices de l'OCDE régissant la protection de la vie privée[56]. Par ailleurs, les Etats-Unis ont participé activement à l'élaboration de la Déclaration sur l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé[57].

Les Etats-Unis ont adhéré à la Convention de Budapest sur la cybercriminalité[58] du Conseil de l'Europe.

De plus, les Etats-Unis sont membres de la Coopération économique Asie-Pacifique (APEC) et sont partie au Cadre de protection de la vie privée de l'APEC[59].

La FTC est par ailleurs membre accréditée de l'Assemblée mondiale sur la vie privée (*Global Privacy Assembly*)[60] tandis que le PCLOB ainsi que le délégué à la protection des libertés civiles et de la vie privée du DoJ sont observateurs.

Les accords bilatéraux ou plurilatéraux en matière de libre-échange ou de commerce électronique peuvent également être pertinents s'ils contiennent des clauses relatives à la protection des données personnelles et aux flux de données transfrontières. A cet égard, l'accord de libre-échange entre les Etats-Unis, le Mexique et le Canada ainsi que l'accord de libre-échange entre les Etats-Unis et le Japon[61] peuvent notamment être mentionnés. Par ailleurs, les Etats-Unis participent également aux négociations relatives à un accord en matière de commerce électronique menées actuellement sur la base d'une initiative jointe de membres de l'OMC[62].

---

[56] Accessibles sous le lien suivant: OECD Legal Instruments.

[57] Accessible sous le lien suivant: OECD Legal Instruments.

[58] Accessible sous le lien suivant: STCE 185 - Convention sur la cybercriminalité (coe.int), SR 0.311.43.

[59] Accessible sous le lien suivant: APEC Privacy Framework.

[60] C.f. Global Privacy Assembly.

[61] C.f. Digital Trade & E-Commerce FTA Chapters | United States Trade Representative (ustr.gov).

[62] C.f. WTO | Joint Initiative on E-Commerce.

### 5.2 Etat de droit

Les États-Unis sont une république fédérale composée de 50 Etats, auxquels s'ajoutent des territoires non-étatiques. La forme du gouvernement est celle d'une démocratie.

La politique étrangère, l'armée, les activités de renseignement et le commerce extérieur relèvent de l'Etat fédéral. Les 50 Etats fédérés disposent de compétences dans de nombreux domaines, notamment la justice, l'éducation, etc.

La Constitution des Etats-Unis, datant de 1787, est la plus ancienne constitution moderne encore en vigueur. La Constitution consacre la séparation des pouvoirs : le pouvoir législatif est exercé par un Congrès composé de deux chambres, à savoir le Sénat et la Chambre des représentants ; le pouvoir exécutif est assuré par le président et le vice-président des Etats-Unis ; la Cour suprême est la plus haute instance judiciaire aux Etats-Unis, elle entend les affaires des juridictions fédérales inférieures en tant que plus haute cour d'appel ainsi que les affaires portant sur des questions de droit fédéral ou d'interprétation de la Constitution. L'indépendance du pouvoir judiciaire est garantie par la Constitution.

### 5.3 Droits humains

Par ailleurs et pour ce qui est du critère relatif au respect des droits humains, celui-ci doit être perçu par rapport au cadre juridique global d'un Etat, notamment s'agissant de la protection contre toute ingérence disproportionnée dans la vie privée.

La Constitution des Etats-Unis énumère certains droits fondamentaux, qui ne peuvent pas être enfreints par les autorités fédérales ou les autorités des Etats et qui sont appliqués par le pouvoir judiciaire. Ces droits reflètent en partie les droits humains contenus dans la Déclaration universelle des droits de l'homme[63]. C'est notamment le cas de la liberté d'expression, la liberté de croyance, la liberté de réunion, l'égalité et les garanties de procédure.

En outre, des arrêts de la Cour suprême ont abordé la protection des intérêts relatifs à la vie privée dans un certain nombre de contextes, notamment dans le cadre du quatrième amendement, qui établit un droit contre les perquisitions et les saisies déraisonnables par le gouvernement[64].

## 6 Conclusion

Il ressort de ce qui précède que lorsque les autorités d'application du droit pénal ou les autorités de sécurité nationale des Etats-Unis accèdent à des données personnelles transférées depuis la Suisse vers des organisations certifiées, un cadre juridique est en place, définissant les conditions dans lesquelles l'accès peut avoir lieu et garantissant que cet accès et l'utilisation ultérieure des données sont limités à ce qui est nécessaire et proportionné à l'objectif

---

[63] Accessible sous le lien suivant: La Déclaration universelle des droits de l'homme.

[64] C.f. *Griswold v. Connecticut*, 381 US 479 (1965), accessible sous le lien suivant:. Griswold v. Connecticut : 381 US 479 (1965): Justia US Supreme Court Center.

d'intérêt public poursuivi. Ces garanties peuvent être invoquées par les personnes concernées grâce aux voies de droit offertes et sont ainsi effectives.

C'est pourquoi sur la base de l'examen ci-dessus, l'OFJ conclut que les États-Unis assurent un niveau de protection adéquat des données personnelles transférées dans le cadre du *Swiss-U.S. DPF* d'un responsable du traitement ou d'un sous-traitant en Suisse à des organisations certifiées aux États-Unis.

En cas de décision positive du Conseil fédéral prise sur la base de la présente évaluation, les transferts de données entre responsables du traitement ou sous-traitants en Suisse et organisations certifiées aux Etats-Unis pourront avoir lieu sans qu'il soit nécessaire d'obtenir des garanties supplémentaires, conformément aux prescriptions de l'art. 16 al. 1 LPD.

Liens vers les textes de référence :

- Principes, y compris principes supplémentaires, du cadre commercial entre la Suisse et les États-Unis sur la protection des données pour les organisations certifiées, courriers visant à confirmer les engagements pris établis par les autorités suivantes: Département de la justice (DoJ), Département du commerce (Secrétaire au Commerce) (DoC), Administration du commerce international (ITA), Commission fédérale du commerce (FTC) et Département du transport (DoT) ainsi que courrier du bureau de la directrice du renseignement national (ODNI) au DoC: https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3
- Décret exécutif 14086 du 7 octobre 2022: https://www.state.gov/executive-order-14086-policy-and-procedures
- Règlement sur la cour d'examen en matière de protection des données du procureur général des États-Unis (*U.S. Attorney General*) publié le 7 octobre 2022: https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court
- Directive 126 de la communauté du renseignement établie par l'ODNI le 6 décembre 2022: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf
- Désignation de la Suisse le 7 juin 2024 en tant qu'Etat bénéficiant du mécanisme de recours à deux niveaux comprenant l'accès à la cour d'examen en matière de protection des données: https://www.justice.gov/opcl/media/1355326/dl?inline, voir également: https://www.justice.gov/opcl/executive-order-14086