Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Rapport sur le deuxième examen du fonctionnement du bouclier de protection des données Suisse – États-Unis (2019)

I. Introduction

Le 14 septembre 2019 a eu lieu à Washington D.C. le deuxième examen annuel conjoint du bouclier de protection des données Suisse – États-Unis (ci-après : bouclier CH-US) par la délégation suisse et la délégation du gouvernement américain.

Depuis que l'accord sur le bouclier de protection CH-US est entré en vigueur le 17 avril 2017, plus de 3 300 entreprises ont intégré le programme de ce bouclier, avec près de 1000 entreprises certifiées supplémentaires depuis l'examen précédent (octobre 2018). Il s'agit à plus de 70% de PME des secteurs les plus divers, actives notamment dans les domaines des technologies de l'information et de la communication, des services professionnels aux entreprises, des médias et du divertissement, et de la formation. De grands groupes comme Facebook Inc. ou Google LLC sont eux aussi certifiés au titre du bouclier de protection.

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est l'interlocuteur pour les personnes concernées en Suisse et les entreprises.

S'agissant des aspects commerciaux de l'accord, le PFPDT n'a reçu au cours de l'année sous revue qu'une seule réclamation à transmettre au Département du commerce (*Department of Commerce,* DoC), qui concernait une entreprise se faisant passer pour certifiée (*false claim*). L'affaire a pu être résolue en collaboration avec le DoC (cf. ch. 1.4).

En outre, une dizaine de réclamations contre des entreprises certifiées ont été adressées à des organismes privés et indépendants de règlement extrajudiciaire des litiges (ADR). Aucune réclamation concernant des entreprises certifiées ayant choisi le PFPDT comme organisme de réclamation indépendant n'a été introduite. Aucune réclamation concernant des données relatives aux ressources humaines (données RH), obligatoirement soumises au contrôle du PFPDT, n'est à signaler non plus. En revanche, le PFPDT a été consulté plusieurs fois par des entreprises ayant leur siège en Suisse afin de lever certaines incertitudes concernant le transfert de données aux États-Unis.

Depuis la mise en œuvre de l'accord, le PFPDT n'a été saisi d'aucun cas concernant l'accès des autorités américaines aux données personnelles pour des raisons de sécurité nationale.

Il reste difficile de cerner les raisons pour lesquelles les instruments juridiques mis à disposition au titre du bouclier CH-US sont peu utilisés par les personnes concernées en Suisse. Cela pourrait tenir d'une part à la complexité de l'accord et à la difficulté d'identifier d'éventuelles violations des données. Le PFPDT rappelle à cet égard qu'il reste à la disposition des personnes concernées en Suisse et des entreprises pour répondre à leurs questions. Mais il ne faut pas perdre de vue non plus qu'il y a lieu de saisir l'entreprise certifiée avant de recourir éventuellement au PFPDT ou à un ADR, ce qui permet de supposer que certains cas, dont le nombre est toutefois difficile à estimer, ont pu être réglés de cette façon.

Lors du deuxième examen, la Suisse était représentée comme l'an dernier par le Secrétariat d'État à l'économie (SECO), qui conduisait la délégation, et par le PFPDT, en qualité d'autorité spécialisée dans

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

le droit de la protection des données et d'autorité de surveillance. Les États-Unis étaient représentés pour leur part par le DoC.

La rencontre a eu lieu à la suite du 3e examen annuel du fonctionnement du bouclier de protection des données UE – États-Unis (ci-après : bouclier UE-US), auquel la délégation suisse a participé en qualité d'observateur, sans pouvoir prendre la parole. A cette occasion, les États-Unis étaient représentés par les autorités suivantes :

- Département du commerce (*Department of Commerce,* DoC)
- Département d'État (*Department of State,* DoS)
- Commission fédérale du commerce (*Federal Trade Commission,* FTC)
- Département des transports (*Departement of Transportation,* DoT)
- Bureau du directeur du renseignement national (*Office of the Director of National Intelligence,* ODNI)
- Département de justice (*Department of Justice,* DoJ)
- *Privacy and Civil Liberties Oversight Board* (PCLOB; organisme indépendant de contrôle de la protection de la sphère privée et des libertés individuelles)
- Médiateur (et collaborateurs)
- Inspecteur général de la communauté du renseignement (*Inspector General for Intelligence Community*)

L'UE était représentée par :

- la Commission européenne
- huit membres du Comité européen de la protection des données (CEPD)

Eu égard à la grande similitude entre les boucliers suisse et européen, la plupart des thèmes, notamment l'accès aux données personnelles par les autorités américaines ou certains aspects commerciaux de l'accord importants pour la protection des données (par ex. les rapports d'activités de la FTC et du DoT) ont comme l'an dernier été traités exclusivement dans le cadre de l'examen UE – États-Unis (cf. le premier rapport du PFPDT sur le premier examen commun du bouclier CH-US, 2018[1]).

Au niveau de l'UE, la Commission et le CEPD (jusqu'au 25 mai 2018 : Groupe de travail «Article 29» [GT art. 29]) ont tous deux établis leurs propres rapports pour les examens communs précédents (2017[2], 2018[3] und 2019[4]).

---

[1] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html

[2] WP29 : https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf
Commission : https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[3]CEPD :https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en
Commission : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[4] CEPD : https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en
Commission : https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

Le CEPD a tiré ses principaux enseignements en matière de protection des données de la correspondance préalable avec les autorités américaines et du 2e examen commun UE – États-Unis. Ces enseignements sont en grande partie également valables pour le bouclier CH-US. Les autorités américaines procèdent aux ajustements nécessaires en tenant compte de la similitude des deux boucliers.

Le rôle du PFPDT correspond pour l'essentiel à celui du CEPD (précédemment : GT art. 29).

En conséquence, le rapport ci-après répond en grande partie à celui du CEPD.

La Suisse et l'UE reconnaissant comme équivalentes leurs législations en matière de protection des données, la Suisse considère que le niveau de protection du bouclier CH-US est adéquat dans la mesure où l'UE estime que celui du bouclier UE-US l'est aussi.

Alors que le premier examen du bouclier CH-US (2018) avait privilégié la mise en place et le déroulement des procédures prévues par la partie commerciale de l'accord et la prise de contact personnelle avec les représentants américains, l'examen 2019 a également porté sur l'utilisation du bouclier de protection par les entreprises ayant leur siège en Suisse et sur certains ajustements et développements de la partie commerciale.

Pour être complet, il faut encore préciser que l'un des arbitres habitant en Suisse a demandé au cours de l'année sous revue à être radié de la liste. Les autorités américaines ont décidé de ne pas le remplacer pour l'instant. Il est à noter que cette défection ne porte pas atteinte au mécanisme d'arbitrage prévu pour le bouclier CH-US, qui reste pleinement opérationnel[5].

Du point de vue du droit de la protection des données, les aspects suivants sont particulièrement pertinents :

II Examen sous l'angle de la protection des données

1. Aspects commerciaux

1.1. Informations et instructions à l'usage des entreprises américaines

Le niveau de protection des données aux États-Unis n'étant pas jugé équivalent à celui qui prévaut en Suisse, un transfert de données depuis la Suisse vers les États-Unis n'est possible qu'aux conditions prévues à l'art. 6 de la loi fédérale sur la protection des données (LPD ; RS 235.1). Aussi le bouclier de protection doit-il garantir un niveau de protection des données suffisant pour faciliter aux entreprises certifiées le transfert de données vers les États-Unis dans le cadre de l'accord. En conséquence, mais aussi parce que les États-Unis ont une conception de la protection des données qui diffère fondamentalement de celle de la Suisse (et de l'UE), il est essentiel de s'assurer que le texte du bouclier fasse l'objet d'une interprétation uniforme.

C'est pourquoi, et à la demande du GT art. 29 et du CEPD (cf. leurs rapports), le DoC a publié depuis l'entrée en vigueur du bouclier plusieurs directives accessibles et compréhensibles à destination des entreprises certifiées, sous la forme de FAQ (par ex. : (« Accountability for Onward Transfer Principle »[6], « Processing Guidance »[7]). Il a également publié l'an dernier sous la forme de FAQ une notice consacrée aux aspects du bouclier de protection touchant le Royaume-Uni dans le contexte du Brexit[8].

---

[5] Cf. site internet du PFPDT et guide : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html

[6] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs

Le PFPDT salue la démarche proactive adoptée par le DoC en vue de faciliter aux entreprises et aux personnes intéressées la compréhension des mécanismes complexes du bouclier.

Considérant les questions qui lui ont été adressées notamment par des entreprises ayant leur siège en Suisse, le PFPDT se rallie tout particulièrement au souhait du CEPD de voir le DoC préciser plus particulièrement la procédure applicable au traitement des données relatives aux commandes ou l'utilisation de clauses contractuelles types.

1.2. Informations claires et accessibles pour les personnes concernées en Suisse

Comme il a été indiqué au ch. I, les personnes concernées en Suisse et dans l'UE peuvent avoir du mal à faire valoir leurs droits en raison de la complexité du texte régissant le bouclier. À la demande du GT art. 29, puis du CEPD (cf. leurs rapports), les autorités américaines ont, dès la première année d'application et du bouclier UE-US et du bouclier CH-US, publié sur leur site internet des informations aisément compréhensibles sur les droits des personnes concernées, les moyens disponibles et les voies de droit. Les différentes voies de recours sont explicitées et les liens pertinents sont parfois directement indiqués. Au terme des premiers contrôles annuels du texte et en réaction aux propositions du GT art. 29, le DoC a publié sur son site un document d'une page qui présente un aperçu du programme en insistant sur les droits individuels et sur les moyens de les faire valoir[9].

D'autres directives devraient encore être publiées.

On trouvera sur le site du PFPDT des informations supplémentaires sur les droits des personnes concernées en Suisse[10]. Comme il a été indiqué plus haut, il est possible en cas de doute de prendre contact avec le PFPDT par téléphone ou par écrit.

1.3. Autocertification et recertification

S'agissant de l'autocertification et de la recertification, le contrôle par le DoC de la conformité des entreprises avec le bouclier de protection n'a pas connu de modifications par rapport à l'examen du fonctionnement du bouclier de l'an dernier. Lors de la certification comme lors de la recertification, le DoC contrôle les points suivants :

1. enregistrement auprès d'une entreprise au titre du mécanisme de recours indépendant (*Independent Recourse Mechanism*, IRM)
2. versement de la contribution prévue à l'annexe I (*Arbitral Fund Contribution*)
3. respect du principe complémentaire 8 (accès) du bouclier de protection des données
4. intégralité et cohérence des informations relatives à la certification
5. déclaration relative à la protection des données (présence des 13 éléments requis par le bouclier de protection et contrôle de la politique de confidentialité de l'entreprise).

Comme précédemment, le DoC invite au besoin les entreprises à préciser les informations accessibles par des liens, afin de faciliter aux intéressés l'exercice de leurs droits. Il s'assure en outre qu'il n'y ait pas de contradictions entre les indications figurant dans la déclaration de confidentialité des entreprises et celles qui se trouvent sur la liste du bouclier de protection des données (par ex. indications concernant la certification des données RH / non RH). Ces contrôles ont à nouveau permis cette année au DoC de

---

[7] https://www.privacyshield.gov/article?id=Processing-FAQs
[8] https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs
[9] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq
[10] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html

constater que certaines entreprises ne remplissaient pas les exigences prévues et de les écarter en conséquence de la liste des entreprises certifiées. Le DoC continue d'interdire aux entreprises américaines de renvoyer au programme du bouclier de protection des données dans leur déclaration de confidentialité avant qu'il ait terminé le contrôle de leur autocertification et que leur nom soit publié sur la liste du bouclier de protection des données, de façon à prévenir toute contradiction entre les indications figurant dans les déclarations de confidentialité des entreprises et l'état réel de leur première certification.

Si le PFPDT juge ces mesures bienvenues, il n'en continue pas moins, avec le CEPD, de déplorer que les contrôles effectués par le DoC portent principalement sur des critères formels, plutôt que de viser le respect matériel des principes qui fondent le bouclier.

Un contrôle matériel serait pourtant d'autant plus indiqué que la plupart des entreprises se contentent d'une simple auto-évaluation au lieu de faire contrôler la conformité par un service externe.

Comme lors de l'examen du fonctionnement du bouclier UE-US de l'an dernier a été évoqué le problème qui veut que la durée de validité de la première certification expire parfois avant que la procédure de recertification soit achevée, les entreprises concernées figurant alors sur la liste pendant quelque temps sans certification valable. Selon les informations fournies au cours du troisième examen, le processus de recertification peut se prolonger jusqu'à 105 jours après l'échéance effective, les entreprises restant néanmoins répertoriées sur la liste avec le statut « actif ».

Le PFPDT estime à l'instar du CEPD que les personnes privées ne subissent aucun préjudice pendant ce laps de temps, pour autant que les entreprises américaines concernées s'engagent officiellement à continuer de respecter les principes du bouclier de protection des données. Il serait néanmoins souhaitable de pouvoir trouver une solution qui permette de garantir en tout temps la protection des intéressés, de façon qu'aucune incertitude ne subsiste sur ce point. D'ici là, il s'agira de rappeler aux personnes concernées et aux entreprises en Suisse ou dans l'UE qui transmettent des données aux États-Unis de toujours s'assurer de la validité de la certification.

Le troisième examen du fonctionnement du bouclier de protection UE-US a également permis de constater que plusieurs entreprises figurant sur la liste du bouclier possédaient le statut « actif » alors même qu'elles auraient dû être recertifiées en 2018. Aussi le CEPD a-t-il demandé au DoC de mettre en place des procédures qui garantissent que la liste des entreprises au statut « actif » soit toujours à jour.

1.4. Surveillance et contrôle du respect des principes par le DoC

Lors du premier examen du fonctionnement du bouclier de protection UE-US (2017), le GT art. 29 avait critiqué le fait que la surveillance sur les aspects commerciaux du bouclier s'appuyait principalement sur les entreprises qui fournissent des services IRM et que la surveillance et le contrôle opérés d'office par le DoC étaient insuffisants.

L'examen 2018 du fonctionnement du bouclier de protection (le premier pour ce qui est du bouclier CH-US) a permis de constater que la surveillance effectuée par les autorités américaines avait connu des progrès significatifs pour l'un et l'autre boucliers (cf. ch. 1.4 du rapport 2018 du PFPDT).

Selon les informations obtenues cette année, le DoC a porté à 30 par mois le nombre des entreprises choisies au hasard faisant l'objet de contrôles aléatoires et adressé 670 avertissements, notamment à des entreprises se faisant passer pour certifiées. Comme il a déjà été dit dans le rapport précédent, ces améliorations effectuées en vue de garantir le respect formel des principes du bouclier méritent d'être saluées. Mais le CEPD comme le PFPDT regrettent que les contrôles continuent de se concentrer sur les formalités à remplir et non sur le contenu même des principes. C'est pourquoi le CEPD invite à nouveau le DoC dans le cadre du troisième examen UE-US à étendre sa surveillance à des éléments matériels tels que le principe de finalité. De même, en ce qui concerne le transfert de données à des tiers, le DoC n'a par exemple jamais demandé à ce jour de copies des règles de confidentialité figurant dans les

contrats conclus entre des organisations américaines et leurs mandataires (agents). Or, les données peuvent être transférées vers des États tiers qui ne garantissent pas une protection des données adéquate, aussi la responsabilité doit-elle être clairement réglée. Le DoC continue quant à lui d'estimer que si les entreprises qui se font certifier contractent des engagements juridiquement contraignants, cela ne dispense pas pour autant les personnes concernées de faire valoir activement leurs droits. En tout état de cause, le texte du bouclier ne prévoit pas de contrôles plus poussés (cf. ch. 1.4, p. 5, du rapport 2018). Il pourrait cependant être possible d'élargir le champ des contrôles aléatoires.

Comme le CEPD, le PFPDT estime que le DoC devrait procéder à des contrôles plus poussés en vue de vérifier que les entreprises autocertifiées mettent effectivement en œuvre les exigences matérielles du bouclier de protection. Il suivra les développements à venir et continuera d'échanger sur ce point avec les représentants européens et américains.

1.5. Surveillance et contrôle du respect des principes par la FTC

Le deuxième examen conjoint n'a pas permis lui non plus au PFPDT d'avoir un contact direct officiel avec la FTC, celle-ci n'ayant participé qu'à l'examen UE-US, auquel la Suisse a assisté en tant qu'observateur, sans pouvoir poser de questions (cf. ch. I). Les observations faites dans ce cadre valent toutefois par analogie pour l'accord sur le bouclier de protection CH-US.

Depuis le dernier examen du bouclier, la FTC a relevé en tout sept nouveaux cas de non-conformité, qui relevaient tous d'erreurs administratives et non de violations matérielles des principes du bouclier. Le CEPD recommande d'effectuer des contrôles supplémentaires s'agissant de la transmission de données à des tiers, car les solutions mises en place par les entreprises certifiées ne sont pas non plus contrôlées par le DoC.

Dans la division du *Bureau of Consumer Protection* de la FTC chargée de la protection des données et de l'identité, 40 avocats, assistés notamment par des experts techniques, se consacrent quasi exclusivement à la protection des données. S'agissant de l'amende infligée l'an dernier à Facebook, la FTC a précisé que le cadre dans lequel elle s'inscrit se situe hors du champ d'application du bouclier de protection des données.

Le CEPD s'est félicité que la FTC intervienne davantage d'office. Mais comme la FTC ne fournit pas de précisions sur son action, il reste difficile de porter un jugement sur les cas concrets et sur ses activités. Il est donc impossible de se prononcer sur le point de savoir dans quelle mesure elle s'assure effectivement du respect des principes.

1.6. Mécanismes de recours indépendants (IRM)

Le nombre des réclamations adressées aux fournisseurs de services IRM a légèrement augmenté depuis le dernier examen. Mais ces réclamations semblent principalement porter sur des aspects procéduraux et non sur le respect matériel des principes. Aussi l'IRM ne saurait-il se substituer à un renforcement du contrôle matériel par les autorités américaines (cf. ch. 1.4 et 1.5).

Comme il a été précisé dans le rapport 2018, les fournisseurs de services IRM sont tenus d'indiquer dans leurs rapports annuels comment ils entendent éviter les conflits d'intérêts ou les éliminer (cf. ch. 1.6, p. 6, du rapport 2018). Le DoC a fait savoir à cet égard qu'il avait actualisé les directives qu'il avait publiées pour faciliter aux entreprises fournissant des services IRM l'établissement de leurs rapports annuels, en montrant où pouvaient résider les conflits d'intérêts potentiels et comment les éviter. Les directives ne couvrent pas cependant tous les aspects de ces rapports. Le CEPD a notamment constaté que la présentation de ces derniers n'était pas unifiée. Aussi recommande-t-il au DoC d'instituer pour ces rapports annuels un format standard qui permettra une comparabilité parfaite, et prévoyant des précisions sur les mesures prises pour prévenir d'éventuels conflits d'intérêts.

1.7 Données personnelles

Ainsi qu'il avait déjà été indiqué dans le rapport précédent (cf. ch. 1.7 du rapport 2018), la notion de « données personnelles » (ou « données RH ») fait l'objet d'une interprétation différente dans le cadre du bouclier de protection par l'UE et la Suisse d'une part, et les autorités américaines d'autre part. Le DoC et l'UE ont poursuivi l'an dernier les discussions sur leurs divergences d'interprétation quant aux données RH, sans parvenir à trouver un terrain d'entente. Face à ce désaccord sur la définition, les examens de l'an dernier et de cette année se sont moins intéressés à la notion elle-même qu'aux conséquences auxquelles pouvait conduire une différence d'interprétation. Le CEPD et le PFPDT craignent que les mesures de protection supplémentaires prévues par le bouclier pour les données en matière d'emploi qui ne sont pas des données RH (par ex. un consentement explicite [*opt-in*] au lieu d'un consentement implicite [*opt-out*] si les données sont traitées à des fins de marketing) ne soient appliquées par aucune autorité américaine ou européenne. Le PFPDT défend ici le même point de vue que le CEPD, à savoir que des règles plus sévères devraient s'appliquer aux données personnelles, qu'elles soient traitées par l'employeur ou par un sous-traitant (cf. ch. 1.7 du rapport 2018). Les discussions sur ce point se poursuivent entre UE et autorités américaines.

2. Accès aux données personnelles par les autorités au titre de la sécurité nationale

Le cadre juridique américain n'a pas changé fondamentalement depuis le dernier examen. Aussi le GT art. 29, le CEPD et le PFPDT maintiennent-ils les principales réserves qu'ils ont émises dans leurs derniers rapports relativement à l'accès pour motif de sécurité nationale ou de poursuite pénale. Ces réserves concernent plus particulièrement la collecte des données, la surveillance, les voies de droit et le mécanisme du Médiateur. Par ailleurs, il ne faut pas perdre de vue l'affaire Schrems II (C-311/18), actuellement pendante devant la Cour de justice de l'Union européenne (CJUE) et qui touche le bouclier de protection des données UE-US et donc aussi indirectement le bouclier CH-US. L'arrêt devrait être rendu entre mars et mai 2020.

Les représentants américains pour la sécurité nationale étaient uniquement présents à l'examen UE-US, auquel le PFPDT assistait en tant qu'observateur, sans pouvoir prendre la parole. Compte tenu de la similitude des deux boucliers, le PFPDT se rallie pleinement à l'avis du CEPD concernant l'accès aux données par les autorités américaines. Aussi est-il renvoyé au rapport du CEPD du 22 janvier 2019 et à celui du GT art. 29 du 28 novembre 2017 (cf. ch. I).

2.1. Collectes de données pour des motifs de sécurité nationale

2.1.1 Collecte de données au titre de la section 702 du Foreign Intelligence Surveillance Act (section 702 FISA)

Le CEPD rappelle à nouveau qu'il est indispensable de mener sous l'angle de la proportionnalité et de la nécessité une évaluation indépendante sur ce qu'il faut entendre par « cibles » et par « intelligence étrangère » au sens de la section 702 FISA (y compris dans le cadre du programme UPSTREAM). Il demande d'autre part à nouveau que soit également menée une évaluation indépendante sur l'utilisation de mots-clefs dans le cas particulier (« *tasking of Selectors* », par ex. téléphone, adresse électronique, etc.). Il continue enfin de demander des éclaircissements sur le programme de surveillance UPSTREAM afin de s'assurer qu'il ne soit pas procédé arbitrairement à des collectes massives de données personnelles de personnes non US au sens de la section 702 (cf. ch. 2.1 du rapport 2018).

S'agissant de la section 702 FISA, l'examen de cette année a permis de préciser qu'une personne à identifier au titre de « cible » pouvait correspondre à plusieurs personnes ayant le même identifiant, pour autant que ces personnes soient toutes des personnes non US et qu'elles remplissent les critères applicables au ciblage.

Le CEPD se félicite que le PCLOB, désormais pleinement opérationnel, ait décidé en sa qualité d'autorité de surveillance indépendante d'examiner la consultation par le FBI des données collectées en vertu de la section 702, et qu'il ait indiqué vouloir s'assurer que les recommandations qu'il avait faites précédemment dans le rapport qu'il avait consacré à la section 702 avaient effectivement été suivies d'effet, et dans quelle mesure. Le CEPD regrette cependant que le PCLOB n'ait pas l'intention d'établir et de publier un rapport complet actualisé sur la section 702 et s'appuyant sur le rapport présenté en 2014. Un tel rapport contribuerait en effet à procéder à une évaluation des nouvelles dispositions de la section 702 (nouvelle autorisation de la section 702 votée en 2017) et des procédures de services de renseignement.

2.1.2. Collecte de données au titre du décret présidentiel 12333 (Executive Order 12333, ou EO 12333)

Le CEPD maintient que l'adéquation du niveau de protection des données ne doit pas se limiter à la surveillance à l'intérieur des frontières physiques ou géographiques d'un État tiers. Il y a lieu en effet d'analyser également les bases légales qui permettent à cet État de procéder à une surveillance hors de son territoire portant sur des données de citoyens de l'UE (ou suisses). Les restrictions auxquelles est soumis l'accès des autorités aux données personnelles devrait être étendu aux données qui sont « en route » pour un pays pour lequel un niveau adéquat a été reconnu.

Les autorités américaines ont souligné à l'occasion du dernier examen que l'EO 12333 ne pouvait servir de base légale pour la collecte de données sur le territoire américain et que la collecte de données dans le cadre de l'EO 12333 n'entrait pas dans le champ d'application du bouclier de protection des données (cf. ch. 2.1 du rapport 2018 du PFPDT).

Face à l'incertitude et l'imprévisibilité qui continuent d'entourer l'application de l'EO 12333, le CEPD a insisté à nouveau sur la nécessité de voir le PCLOB établir des rapports qui éclairent ce texte. Il est cependant probable que ces rapports resteront secrets et que ni le grand public ni les représentants des États tiers n'auront accès à des informations supplémentaires sur le fonctionnement concret de l'EO 12333 (pas plus que sa nécessité et sa proportionnalité).

2.1.3. Mesures de protection prévues par la Presidential Policy Directive 28 (PPD-28)

Le CEPD se félicite que les autorités américaines confirment l'application (en principe) de la PPD-28 (cf. rapport 2018 du PFPDT), notamment parce qu'elle est la seule à prévoir des garanties et des restrictions pour la collecte et l'utilisation de données hors des États-Unis (car les restrictions du FISA ou d'autres lois américaines plus spécifiques ne s'appliquent pas à cet égard).

La PPD-28 restreint l'utilisation de la collecte massive de données à six finalités de sécurité nationale (détection et neutralisation des menaces d'espionnage, terrorisme, armes de destruction massive, cyber sécurité, menaces contre les forces armées et menaces criminelles transnationales), afin de mieux protéger la vie privée de tous, y compris des citoyens non américains. Le troisième examen du bouclier UE-US n'a pas donné lieu à de nouveaux échanges de fond sur l'interprétation et l'application de ces six finalités qui auraient permis d'évaluer les assurances données par les autorités américaines.

Les autorités américaines font certes valoir que les décrets présidentiels et les *Presidential Policy Directives* sont d'« application obligatoire », mais il ne faut pas perdre de vue que ces instruments juridiques ne fondent aucun droit justiciable. Il serait ainsi impossibles pour une personne concernée en Suisse ou dans l'UE d'invoquer directement une violation de la PPD-28 (cf. ch. 2.3 du rapport 2018 du PFPDT).

2.2. Surveillance sur les programmes de surveillance des autorités américaines

Le CEPD rappelle qu'il est essentiel d'exercer un contrôle global sur les programmes de surveillance.

Les deux derniers examens annuels conjoints avaient déjà donné lieu à la présentation des activités de surveillance de plusieurs institutions ou organes. Le CEPD estime qu'il a été mis en place une architecture globale de surveillance composée d'organes divers et pour certains d'entre eux indépendants de la communauté du renseignement, parmi lesquels les *Privacy and Civil Liberty officers*, les *Inspector Generals*, le PCLOB, la *Foreign Intelligence Surveillance Court* du Congrès (FISC ; Cour de Surveillance du Renseignement Étranger).

Le CEPD salue également la nomination des derniers membres encore manquants du PCLOB, qui est désormais pleinement opérationnel. Le PCLOB a présenté pour la première fois son programme de travail, et le CEPD a émis une appréciation positive sur la transparence de cet organe de surveillance. Pour le CEPD, le PCLOB constitue un élément indépendant important de l'« architecture de surveillance ».

Le CEPD demande cependant à nouveau que soient publiés ou actualisés certains rapports (section 702 FISA, PPD-28).

De manière générale, il faut relever qu'il n'est guère possible de mener une évaluation valable de la surveillance exercée sur les programmes de surveillance des autorités américaines, les représentants des États tiers ayant uniquement accès aux documents publics.

2.3. Voies de recours pour les personnes concernées suisses

Comme il a déjà été indiqué l'an dernier (cf. ch. 2.3 du rapport 2018), pour pouvoir être certaines qu'un État tiers dispose d'un niveau adéquat de protection des données, il est essentiel que les personnes concernées en Suisse puissent avoir accès à un organisme de réclamation indépendant et impartial.

Les autorités américaines ayant fait savoir que le cadre juridique n'avait pas connu de modification depuis le dernier examen, le lecteur est renvoyé aux explications auxquelles celui-ci a donné lieu (cf. ch. 2.3 du rapport 2018 du PFPDT).

Comme précédemment, l'interprétation très restrictive des exigences procédurales (« *standing requirements* ») rend irréaliste un contrôle juridictionnel des opérations de surveillance (section 702 FISA, EO 12333, etc.). Il a été confirmé à l'occasion des rapports UE-US que l'interprétation du terme « *standing* » en matière de surveillance est en train d'évoluer, les affaires concernées étant encore pendantes[11].

2.4. Mécanisme du Médiateur

Le CEPD a salué à l'occasion du troisième examen UE-US la nomination, le 18 janvier 2019, de M. Keith Krach au poste de médiateur « permanent ».

Le mécanisme du Médiateur étant à l'heure actuelle pratiquement le seul moyen direct de faire contrôler le respect des principes du droit de la protection des données (PPD-28, EO 12333, section 702 FISA, etc.) par les autorités américaines, il est essentiel que le Médiateur soit indépendant et impartial.

En sa qualité de sous-secrétaire d'État à la Croissance économique, à l'Énergie et à l'Environnement. M. Krach est certes indépendant des services de renseignement, mais non du gouvernement américain.

S'agissant des plaintes déposées par les personnes concernées, les médiateurs et le gouvernement américain ont indiqué lors du dernier examen comment ils procédaient pour s'assurer qu'elles fassent l'objet d'un traitement efficace et conforme au droit. Les collaborateurs du Médiateur ont ainsi expliqué à la lumière d'un cas théorique comment les plaintes étaient traitées (cf. ch. 2.4 du rapport 2018).

[11] Cf. notamment les affaires ACLU contre Clapper et Wikipedia contre NSA.

M. Krach a confirmé les propos du dernier médiateur, indiquant qu'il ne signait une décision de classement que lorsqu'il était certain qu'elle avait été dûment traitée, et qu'il n'hésitait pas à la porter devant le niveau le plus élevé du service américain compétent si la conclusion proposée ne l'avait pas convaincu.

Les procédures qui régissent l'accès du Médiateur aux information pertinentes et les interactions des différents organes de la communauté du renseignement, y compris les autorités de surveillance, sont en partie secrètes, ce qui complique considérablement leur évaluation.

Même s'il n'existe pas d'indices concrets permettant de douter de l'intégrité du nouveau Médiateur, le CEPD n'en demande pas moins à pouvoir disposer d'informations supplémentaires sur les pouvoirs du Médiateur vis-à-vis de la communauté du renseignement.

Les informations disponibles ne permettent toujours pas à ce jour d'affirmer que les prérogatives du Médiateur à l'égard des services de renseignement sont suffisantes, puisqu'en cas de violation du droit, ses « pouvoirs » semblent se limiter à refuser de confirmer que les droits fondamentaux du requérant ont été respectés. À quoi s'ajoute que ses décisions ne peuvent faire l'objet d'un recours en justice.

Cet état de fait est problématique, notamment au regard du droit fondamental à porter sa cause devant un tribunal indépendant et impartial.

III. Conclusion

Le PFPDT salue les efforts consentis par les autorités américaines pour améliorer le programme du bouclier de protection des données, notamment en ce qui concerne les mesures de surveillance et de mise en œuvre prises d'office et la nomination des derniers membres manquants du PCLOB et du Médiateur permanent.

Des améliorations restent néanmoins possibles. Par ex., s'agissant des aspects commerciaux, la mise en œuvre de contrôles matériels par le DoC, le respect des exigences applicables à la transmission de données à des tiers ou la problématique non encore résolue des données RH continuent de figurer parmi les préoccupations du CEPD comme du PFPDT.

En ce qui concerne la collecte des données par les autorités américaines, il serait notamment utile de disposer de rapports, ainsi sur les garanties de la PPD-28.

Pour ce qui est du mécanisme du Médiateur, les informations fournies à l'occasion de l'examen UE-US ne permettent pas d'affirmer que le Médiateur dispose de pouvoirs suffisants pour avoir accès à toutes informations nécessaires et remédier à une violation des règles de la protection des données. En conséquence, pour le bouclier CH-US non plus, il n'est pas possible à ce jour de certifier que le mécanisme du Médiateur soit de nature à répondre aux exigences qui caractérisent une autorité de recours impartiale.

Rappelons enfin ici qu'il s'agit encore d'attendre l'issue des affaires pendantes devant la CJUE, notamment l'affaire « Schrems II », qui auront indirectement des incidences pour la Suisse.