Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Rapport sur le 1er examen du fonctionnement du bouclier de protection des données Suisse-États-Unis (2018)

I. Introduction

L'examen annuel conjoint du fonctionnement du bouclier de protection des données Suisse-États-Unis (Swiss-US Privacy Shield ; ci-après bouclier de protection CH-US) est prévu par l'accord entre la Suisse et les États-Unis sur le bouclier de protection des données, entré en vigueur le 17 avril 2017. Le premier examen conjoint de la délégation suisse et de la délégation du gouvernement américain a eu lieu à Bruxelles le 20 octobre 2018.

2883 entreprises américaines ont intégré le programme du bouclier de protection CH-US, dont Facebook, Inc., Microsoft Corporation avec 27 filiales (*covered entities*) et Google LLC (état : février 2019).

Au cours de l'année sous revue, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a reçu deux réclamations de la part des personnes concernées concernant des entreprises se faisant passer pour certifiées (*false claims*). Les deux cas ont pu être résolus en collaboration avec le Département du commerce américain (DoC) (cf. ch. 1.4).

En outre, environ dix 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.

A ce jour, le PFPDT n'a pas reçu non plus de réclamation en matière d'accès aux données personnelles par les autorités américaines, au titre du mécanisme du Médiateur.

On pourrait en conclure que les instruments juridiques mis à disposition au titre du bouclier de protection CH-US sont peu utilisés. On notera toutefois que le bouclier n'est en vigueur que depuis avril 2017. En outre, il faudrait saisir l'entreprise certifiée avant de recourir éventuellement à un ADR. On peut donc supposer qu'un certain nombre de cas, difficile à estimer, est déjà réglé par cette voie.

Lors du premier examen, la Suisse était représentée par le Secrétariat d'État à l'économie (SECO), qui conduisait la délégation et par le PFPDT, en qualité d'autorité de surveillance. Les États-Unis étaient représentés par le DoC.

La rencontre a eu lieu à la suite du 2e examen annuel du fonctionnement du bouclier de protection des données UE - États-Unis, auquel la délégation suisse a participé en qualité d'observateur, sans pouvoir poser de questions. A cette occasion, les États-Unis étaient représentés par les autorités suivantes :

- DoC,
- Département d'État (DoS),
- Commission fédérale du commerce (FTC),
- Département des transports (DoT),

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

- Bureau du directeur du renseignement national (ODNI),
- Département de 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 en fonction (et collaborateurs),
- Inspecteur général de la communauté du renseignement

L'UE était représentée par:

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

Le contexte et la teneur des boucliers suisse et européen sont quasiment identiques. La plupart des thèmes, notamment l'accès aux données personnelles par les autorités américaines et différents aspects commerciaux de l'accord (par ex. la définition des données RH et les rapports d'activités de la FTC et du DoT) ont par conséquent été traités exclusivement dans le cadre de l'examen UE - États-Unis.

Le rôle du PFPDT correspond pour l'essentiel à celui du CEPD (jusqu'au 25 mai 2018: Groupe de travail «Article 29» [GT art. 29]).

Le CEPD a tiré ses principaux enseignements de la correspondance préalable avec les autorités américaines et du 2e examen commun UE – États-Unis. Ces enseignements peuvent en grande partie être repris tels quels pour le bouclier CH-US. La Suisse et l'UE reconnaissant comme équivalente leur législation 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 – États-Unis l'est aussi.

Au niveau de l'UE, tant la Commission que le CEPD ont rédigé un rapport en 2017 et en 2018 concernant les deux premiers examens communs réalisés à ce jour[1].

Le PFPDT et les autorités de protection des données de l'UE se sont concertés afin de coordonner la préparation et la finalisation de l'examen. Le présent rapport et celui du CEPD se recoupent donc dans une large mesure.

Pour la Suisse, le premier examen a permis d'établir un contact personnel avec le DoC. En outre les cinq arbitres habitant en Suisse du bouclier CH-US, qui complètent la liste de l'UE, ont pu être officiellement nommés avant le premier examen CH-US. Les noms des cinq arbitres supplémentaires ont été ajoutés à la liste de l'*International Centre For Dispute Resolution* de l'*American Arbitration Association* (ICDR/AAA) avant ceux des arbitres nommés par l'UE. Le mécanisme d'arbitrage du bouclier CH-US est donc pleinement opérationnel[2].
L'établissement et la mise en service des éléments convenus dans le cadre du bouclier CH-US, de même que leur fonctionnement et leur développement ont été discutés lors du premier examen. La Suisse a pu tirer profit du premier examen mené en 2017 par l'UE et les États-Unis concernant leur bouclier de protection, en vigueur depuis le 12 juillet 2016. Plusieurs recommandations émises par l'UE lors de l'examen de 2017 ont été mises en œuvre par les autorités américaines également pour le bouclier

[1] https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
[2] Cf. site Internet du PFPDT et guide:
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/ueber-mittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html

CH-US. S'agissant des aspects commerciaux, le DoC a notamment donné suite à l'exigence de la Commission européenne de rechercher activement les entreprises qui se prétendent certifiées au titre du bouclier de protection. Au surplus, le DoC contrôle plus régulièrement qu'au début les entreprises certifiées afin de détecter d'éventuelles faiblesses concernant le respect des principes.

Concernant l'accès aux données personnelles par des autorités américaines, les représentants du CEPD ont relevé, à l'occasion de l'examen UE-États-Unis de 2018, que les autorités américaines avaient publié des documents utiles à la compréhension des collectes de données depuis l'examen de 2017. La discussion menée lors du 2e examen a contribué à améliorer la compréhension des programmes de surveillance et la transparence (par ex. décisions concernant la *Foreign Intelligence Surveillance Court* [FISA Court]).

Du point de vue de l'autorité de surveillance, 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

La Suisse et l'Europe ont une conception de la protection des données fondamentalement différente de celle des États-Unis. Afin d'éviter autant que possible que les principes du bouclier de protection donnent lieu à des interprétations différentes, ceux-ci doivent être clairs et univoques. La plupart des entreprises américaines qui s'autocertifient procèdent à une auto-évaluation et ne font pas contrôler leur conformité par des services externes. Les règles à respecter sont complexes, particulièrement celles qui s'appliquent au transfert de données à des tiers (*Onward Transfer*). En 2018, le PFPDT a reçu de nombreuses demandes à ce sujet de la part d'entreprises suisses qui transfèrent des données aux États-Unis. Lors du 1er examen en 2017, l'UE a exigé que les entreprises disposent d'instructions claires et d'informations compréhensibles. Le DoC a donné suite à cette exigence et publié une foire aux questions concernant l' *Accountability for Onward Transfer Principle* sur son site Internet[3]. D'autres instructions sont attendues.

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

Les personnes concernées en Suisse (et dans l'UE) peuvent avoir du mal à faire valoir leurs droits en raison de la complexité du cadre du bouclier de protection des données. Des informations claires, compréhensibles et facilement accessibles sont donc indispensables. Le DoC a publié sur son site dédié au bouclier de protection des informations à l'usage des personnes concernées et un aperçu du programme sous la section « EU and Swiss Individuals »[4] [5].

D'autres informations concernant les droits des personnes concernées en Suisse sont disponibles sur le site du PFPDT[6].

[3] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs
https://www.privacyshield.gov/article?id=Processing-FAQs
[4] https://www.privacyshield.gov/Individuals-in-Europe
[5] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq
[6] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html

1.3. Autocertification et recertification

Les entreprises américaines adhérent au boulier de protection des données au moyen d'une simple auto-évaluation, sans recourir à un contrôle de la conformité par un service externe, comme nous l'avons vu plus haut. Il importe donc que le DoC contrôle le respect des principes de la protection des données lors de la certification et de la recertification. Depuis l'entrée en vigueur du bouclier de protection des données, les autorités américaines ont procédé à des améliorations à cet égard. Lors de la certification comme lors de la recertification, le DoC contrôle désormais les points suivants :

1. enregistrement auprès d'une entreprise au titre du mécanisme de recours indépendant (IRM),
2. versement de la contribution prévue à l'annexe I (*Arbitral Fund Contribution*),
3. respect du principe complémentaire 6 (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).

Au besoin, le DoC invite les entreprisses à préciser les informations accessibles par des liens. Il contrôle en outre les éventuelles contradictions entre les indications figurant dans la déclaration de confidentialité des entreprises et la liste du bouclier de protection des données (par ex. indications concernant la certification des données RH / non RH).

Selon les indications données par le DoC lors de l'examen UE – États-Unis, plusieurs entreprises ont été rejetées à l'issue de ces contrôles pour non-respect des principes.

Au chapitre des améliorations considérables, il convient de noter que Le DoC interdit depuis peu aux entreprises de renvoyer au programme du bouclier de protection des données dans leur déclaration de confidentialité avant qu'il ait terminé le contrôle de leur auto-certification et que leur nom soit publié sur la liste du bouclier de protection des données. Les renvois prématurés à l'adhésion au bouclier de protection des données doivent être retirés des sites Internet, ce qui permet d'éviter les contradictions entre les indications figurant dans les déclarations de confidentialité des entreprises et l'avancement réel de leur première certification.

La recertification a également été discutée à l'occasion du 2^{e} examen UE-États-Unis. Il est arrivé que la durée de validité de la 1re certification expire avant que la procédure de recertification soit achevée. Les entreprises concernées ont donc figuré sur la liste pendant quelque temps sans certification valable. Le PFPDT et le CEPD estime que les personnes privées ne subissent aucun préjudice pendant ce laps de temps, pour autant que les entreprises américaines concernées s'engagent officiellement à respecter en tout temps les principes du bouclier de protection des données. Il serait néanmoins souhaitable qu'on puisse totalement exclure qu'une entreprise américaine ne respecte pas absolument le programme.

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

Le DoC a considérablement amélioré la surveillance du respect des principes du bouclier de protection des données par les entreprises américaines depuis le 1er examen UE-États-Unis, ce dont l'accord avec la Suisse profite aussi. En effet, dans le cadre du bouclier de protection des données CH-US, le DoC fera d'office ce qui suit :

- Rechercher, sur une base trimestrielle, les entreprises se faisant passer pour certifiées.

  Jusqu'ici, le PFPDT a reçu deux réclamations de la part des personnes concernées portant sur des entreprises se faisant passer pour certifiées. Les deux cas ont pu être résolus en collaboration avec le DoC.

- Lorsqu'une entreprise est identifiée comme non conforme, le DoC lui adresse un courrier indiquant qu'elle sera signalée à la FTC/au DoT si elle persiste à ne pas respecter les exigences ou ne retire pas la mention du programme du bouclier de protection des données. L'entreprise doit répondre dans les 30 jours. Le DoC tient une liste des entreprises qui ne donnent pas suite à son courrier.

- Le DoC procède en outre à des recherches aléatoires sur Internet.

- Le DoC a contrôlé 100 entreprises (y compris des entreprises adhérant au bouclier UE-US) de manière aléatoire. Le contrôle a porté en particulier sur l'accès à la déclaration de confidentialité, la disponibilité de l'entreprise à se mettre en conformité et la disponibilité de l'IRM.

- Une personne est chargée de faire des recherches par mots-clés dans les médias afin d'identifier les éventuelles violations du cadre du bouclier de protection des données.

- Le DoC vérifie régulièrement que les liens vers les déclarations de confidentialité des entreprises figurant sur la liste du bouclier de protection des données ne sont ni morts ni brisés.

Lors du 2e examen UE-États-Unis, le CEPD s'est félicité de ces nouvelles mesures de surveillance mais a toutefois déploré que les contrôles se limitent aux aspects formels. Des contrôles matériels s'imposent. Le respect des principes, en particulier en ce qui concerne le transfert de données à des tiers, est capital. Jusqu'ici, le DoC n'a par exemple jamais demandé 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 estime quant à lui que le bouclier de protection des données n'exige pas de contrôles aussi poussés.

Lors du 1er examen CH-US, le DoC a fait comprendre au PFPDT qu'à son sens l'accord sur le bouclier de protection des données a valeur de loi et qu'il est donc contraignant pour les entreprises certifiées mais que les personnes concernées ne sont pas pour autant dispensées de faire valoir activement leurs droits. En conséquence, le DoC entreprend généralement des vérifications sur des entreprises américaines sur réclamation.

Le PFPDT partage l'avis du CEPD, selon lequel les autorités américaines devraient procéder à des contrôles d'office. En effet, au vu de la complexité des traitements de données, lesquels ne sont d'ailleurs pas toujours évidents, il peut être extrêmement difficile pour les personnes concernées de faire valoir leurs droits.

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

Lors du 1er examen conjoint, le PFPDT n'a pas eu de contact direct avec la FTC, celle-ci n'ayant participé qu'à l'examen UE-États-Unis, 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 1er examen UE-États-Unis, la FTC a intensifié ses activités de surveillance et de contrôle du respect des principes du bouclier de protection des données.

Selon les indications de la FTC, 40 avocats s'occupent désormais presqu'exclusivement du domaine « protection des données ». Ceux-ci sont en outre soutenus notamment par des experts techniques.

La FTC a signalé quelques nouveaux cas de non-respect des principes du bouclier de protection des données. Le PFPDT ignore toutefois si les entreprises concernées adhéraient également au bouclier CH-US.

A titre expérimental, la FTC a envoyé des injonctions administratives (*Civil Investigative Demands*) à des entreprises, aux fins de vérifier le respect des principes du bouclier de protection des données. Elle n'a cependant révélé ni ses cibles ni le contenu de ses formulaires. La FTC dispose d'une large marge de manœuvre dans ses activités de surveillance. Elle peut agir sans soupçon concret.

A l'instar du CEPD, le PFPDT se félicite que la FTC agisse davantage d'office. Toutefois, celle-ci n'ayant fourni aucun détail, toute évaluation des cas concrets et de ses activités est impossible. Il est également impossible de juger de l'ampleur effective de ses contrôles du respect des principes.

1.6. Mécanismes de recours indépendants

Le DoC a publié des directives afin d'harmoniser et de rendre plus lisibles les rapports annuels des entreprises fournissant des services IRM. Ces directives mettent également en évidence les éventuels conflits d'intérêts des entreprises qui vérifient d'office la conformité et fournissent des services IRM aux mêmes entreprises. Les fournisseurs de services IRM sont tenus d'indiquer dans leurs rapports annuels comment ils entendent éviter de tels conflits d'intérêts ou les éliminer.

1.7 Données personnelles

Les autorités américaines ont une conception différente des « données personnelles » (données RH) de celle des représentants de la Suisse et de l'UE. Cette interprétation différente a déjà été discutée lors de l'examen UE-États-Unis de 2017 et analysée de manière approfondie dans le rapport du « GT art. 29 » qui a suivi. Selon le DoC, seules les données d'employés qui sont transférées dans la même entreprise aux États-Unis sont des données RH. Les données personnelles d'une entreprise suisse (ou de l'UE) qui sont transférées à un mandataire certifié au titre du bouclier aux États-Unis ne sont pas des données RH, selon cette interprétation, mais des données clients. Ces dernières ne bénéficient pas du niveau de protection plus élevé que le cadre du bouclier de protection des données prévoit pour les données RH (lesquelles sont par ex. obligatoirement soumises au contrôle du PFPDT, qui peut adresser des injonctions aux entreprises américaines).

Le PFPDT partage l'opinion du « GT art. 29 » (et du CEPD), selon laquelle on entend par données RH les données personnelles qui, dans l'UE et en Suisse, sont traitées dans le cadre d'un rapport de travail, peu importe qu'elles soient traitées par l'employeur ou par un sous-traitant. Les données RH ne peuvent être transférées sans autre formalité à une entreprise américaine que si la certification de celle-ci au titre du bouclier de protection des données couvre également les données RH. Le PFPDT estime que toutes les données concernant des employés collectées en Suisse doivent jouir d'une protection particulière. En raison du rapport de subordination existant, l'employé ne peut pas vraiment décider librement de révéler ou non ses données personnelles. Il importe donc que celles-ci jouissent de la protection accrue prévue lors de leur traitement ultérieur (par ex. un consentement *explicite* au lieu d'un consentement *implicite* si les données sont traitées à des fins de marketing).

Les autorités de l'UE et des États-Unis n'ont pas réussi jusqu'ici à éliminer leurs divergences d'interprétation. La définition des données RH a été discutée lors de l'examen UE-États-Unis de 2017. Lors de l'examen de 2018, ce sont les conséquences des divergences d'interprétation qui ont été discutées. Les représentants de l'UE se sont notamment inquiétés du fait que les règles plus restrictives en matière de protection des employés, garanties par l'accord sur le bouclier de protection des données, ne peuvent

pas être appliquées. A l'occasion de l'examen CH-US, le PFPDT a signalé au DoC qu'il se ralliait entièrement à l'appréciation du CEPD.

2. Accès aux données personnelles par les autorités / sécurité nationale

Les représentants des États-Unis responsables de la sécurité nationale n'ont participé qu'à l'examen UE-États-Unis, auquel le PFPDT a assisté en tant qu'observateur. Étant donné que l'UE et la Suisse se garantissent mutuellement un niveau adéquat de protection des données, le PFPDT peut se rallier pleinement à l'avis du CEPD concernant l'accès aux données par les autorités américaines. Nous renvoyons donc au rapport du CEPD du 22 janvier 2019 et à celui du « GT art. 29 » du 28 novembre 2017[7].

2.1. Collectes de données au titre de la section 702 du *Foreign Intelligence Surveillance Act* (section 702 FISA) et du décret présidentiel 12333 *(*Executive Order 12333 ; EO 12333)

Le CEPD exige en particulier des contrôles indépendants contre les collectes de données au titre de la section 702 FISA effectuées de manière arbitraire et les collectes de données en vrac. Il soutient les conclusions du rapport du « GT art. 29 » du 28 novembre 2017, selon lesquelles, des évaluations indépendantes doivent être menées sur la définition des « cibles » et sur « le choix des mots-clefs » (par ex. téléphone, adresse électronique, etc.), du point de vue de la proportionnalité en général et de la nécessité en particulier. LE CEPD déplore qu'aucune mesure de protection supplémentaire pour les personnes concernées de l'UE (et en Suisse) n'aient été mises en œuvre au titre de la directive présidentielle PPD 28, lors de la réactivation de la section 702 FISA à la fin 2017. La PPD 28 prévoit entre autres que l'accès aux données doit être aussi ciblé que possible (« *as tailored and as feasible as possible* »). Elle prévoit également des garanties concernant les données personnelles de tous les particuliers, indépendamment de leur nationalité et de leur domicile. Elle restreint en outre le recours à la collecte de données en vrac à six domaines de protection.

S'agissant des surveillances, pour lesquelles des données personnelles sont collectées hors des États-Unis (au titre de l'EO 12333), le CEPD renvoie aux observations faites par le « GT art. 29 » lors du 1er examen UE-États-Unis. Selon le CEPD, pour que l'adéquation du niveau de protection des données d'un État tiers soit garantie, il ne suffit pas que le traitement des données soit adéquat dans cet État, il faut également que les règles qui permettent à cet État de traiter des données hors de son territoire le soient aussi, si des données personnelles de citoyens de l'UE (ou suisses) sont concernées.

Les autorités américaines estiment quant à elles que les traitements de données effectuées au titre de l'EO 12333 ne sont pas couvertes par le bouclier de protection, puisque l'EO 12333 ne permet pas de traiter des données **à l'intérieur** des États-Unis. Compte tenu de l'incertitude et de l'imprévisibilité entourant la mise en œuvre de l'EO 12333, le CEPD renvoie au rapport du « GT art. 29 » de 2017. Il se félicite que les autorités américaines confirment l'application (en principe) de la PPD 28. Toutefois, après avoir analysé les informations fournies par les autorités américaines sur la PPD 28, il arrive à la conclusion que ni le rapport du PCLOB sur la PPD 28, ni le 2e examen UE-États-Unis n'ont apporté de nouvelles informations sur l'interprétation du texte de la PPD 28. Il mentionne notamment des ambiguïtés concernant l'interprétation des six domaines mentionnés plus haut et estime qu'un rapport de suivi détaillé sur la mise en œuvre de la PPD 28 dans les différents programmes de surveillance serait souhaitable. Il se-

[7] https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf

rait également souhaitable que le rapport sur l'EO 12333 que le PCLOB doit encore finaliser informe notamment sur l'applicabilité concrète, la nécessité et la proportionnalité des collectes de données qui se fondent sur cette directive.

2.2. Surveillance sur les programmes de surveillance des autorités américaines

LE CEPD souligne l'importance de la surveillance sur les programmes de surveillance des autorités américaines. Lors de l'examen UE-États-Unis de 2017, les opérations de surveillance de différentes institutions américaines ont été présentées. D'autres organes ont été présentés lors du 2e examen, ce qui a permis de mieux comprendre le fonctionnement des Inspecteurs généraux (organes de surveillance).

LE CEPD estime que les organes de surveillance compétents (PCLOB, organe de surveillance du département de justice et inspecteurs généraux) sont suffisamment indépendants de la communauté du renseignement.

Le CEPD estime que le PCLOB est un élément essentiel de la surveillance sur les autorités américaines. Lors du 1er examen UE-États-Unis, le « GT art. 29 » avait demandé la nomination des quatre membres manquants du PCLOB. Le 11 octobre 2018, le Sénat américain a confirmé la nomination du nouveau président Adam Klein et de deux autres membres : le quorum est ainsi atteint et le PCLOB peut désormais délibérer et décider valablement. Cela lui permet d'exercer ses fonctions en tant qu'organe de surveillance indépendant. Des sièges restent toutefois à pourvoir.

2.3. Voie de recours pour les personnes concernées suisses

Dans son arrêt Schrems, pertinent pour le bouclier de protection des données UE-États-Unis (et indirectement pour le bouclier CH-US), la Cour de justice de l'Union européenne (CJUE) constate qu'en vertu de l'art. 47 de la Charte des droits fondamentaux de l'Union européenne, toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal national. Cela signifie que toute personne doit pouvoir exercer des voies de droit afin d'avoir accès à des données à caractère personnel la concernant, ou d'obtenir la rectification ou la suppression de celles-ci.

La Constitution fédérale (Cst.) garantit aussi que toute personne a droit à ce que sa cause soit portée devant un tribunal établi par la loi, compétent, indépendant et impartial (art. 29 ss Cst.). Pour que le niveau de protection d'un État tiers puisse être considéré comme adéquat, cet État doit mettre à disposition un tribunal devant lequel un recours effectif puisse être introduit.

La PPD 28 ne fonde aucun droit justiciable. Aucune voie de recours n'existe contre une surveillance électronique illicite fondée sur l'EO 12333. A l'heure actuelle, l'interprétation très restrictive des dispositions procédurales rend irréaliste un contrôle juridictionnel des opérations de surveillance au titre du FISA. Pour la Cour Suprême des États-Unis, le danger abstrait d'une surveillance ne suffit pas à justifier un contrôle juridictionnel, il faut apporter la preuve que les communications ont été surveillées.

Il est donc extrêmement difficile pour un Suisse (ou un citoyen de l'UE) de recourir contre des mesures de surveillance devant un tribunal ou de demander un contrôle juridictionnel de celles-ci. Cette situation est problématique au regard de la garantie du droit fondamental à une protection juridique efficace. L'évolution de l'interprétation de la qualité pour agir dans le domaine de la surveillance (aussi dans les procédures en cours) doit être suivie[8]

[8] Cf. rapport du CEPD du 22 janvier 2019, ch. 4.4, p. 18, et les affaires ACLU v. Clapper et Wikipedia v. NSA.

A l'heure actuelle, le mécanisme du Médiateur est pratiquement le seul moyen (direct) dont dispose une personne concernée en Suisse pour faire contrôler le respect des principes du droit de la protection des données (PPD 28, EO 12 333, section 702 FISA, etc.) par les autorités américaines. Il importe donc que les principes procéduraux de ce mécanisme satisfassent à des exigences élevées, analysées ci-après.

2.4 Le Médiateur

L'accès au mécanisme du Médiateur a été mis en œuvre l'année suivant l'entrée en vigueur du bouclier de protection des données CH-US. Le PFPDT, à l'instar des représentants du CEPD (et du « GT art. 29 ») estime que la création du mécanisme du Médiateur, qui permet aux personnes concernées de recourir contre l'accès à leurs données personnelles par les autorités américaines, est réjouissante. Il examine les plaintes, si nécessaire avec le PCLOB, et, s'il constate une violation des droits de la personnalité, s'adresse à l'Inspecteur général (indépendant) du service de renseignement concerné, lequel contrôle les directives internes de l'autorité (ou le bureau compétent de protection de la vie privée et des libertés).

Compte tenu des garanties de procédure inscrites dans la Constitution fédérale, le Médiateur doit satisfaire à des exigences élevées en matière d'indépendance et d'impartialité.

Le 28 septembre 2018, Manisha Singh, Acting Under Secretary of State for Economic Growth, Energy, and the Environment, a été nommée Médiateur par intérim. Elle a remplacé Judith Graber (secrétaire d'État adjointe aux océans et aux affaires environnementales et scientifiques internationales par intérim auprès du Département d'État).

Lors du 2e examen conjoint du bouclier de protection des données UE-États-Unis, le Médiateur et d'autres représentants américains ont expliqué le fonctionnement du mécanisme à la lumière d'un cas théorique. Le Médiateur a assuré qu'il était indépendant des services de renseignement et qu'il traitait les plaintes des personnes concernées efficacement et conformément au droit. Il ne répond toutefois aux requérants qu'après avoir acquis la conviction que la protection des données n'est pas violée. Si nécessaire, il fait usage de la délégation de pouvoirs conférée par le président pour porter le litige au plus haut niveau de l'unité administrative américaine compétente. Selon le Médiateur, les cas concrets doivent demeurer confidentiels. La procédure dans le cas d'espèce et la collaboration entre le Médiateur et la Communauté du renseignement des États-Unis sont en partie secrètes. Tant qu'on n'en saura pas plus sur ces processus, il est impossible de déterminer l'étendue des pouvoirs du Médiateur face aux services de renseignement et de juger si ses compétences sont suffisantes pour se procurer les informations nécessaires et remédier aux problèmes.

A l'heure actuelle, il est par conséquent douteux que des mesures correctrices efficaces puissent être prises en cas d'inobservation des principes garantis de la protection des données. Cet état de fait est problématique, notamment au regard du droit fondamental à porter sa cause devant un tribunal indépendant et impartial, d'autant plus que lors de l'examen UE-États-Unis, il a été confirmé que les décisions du Médiateur ne peuvent pas être portées devant un tribunal.

En outre, le poste de l'Under Secretary, auquel le poste de médiateur est attribué, n'est pas encore pourvu de façon permanente. La désignation d'un Médiateur permanent s'impose donc.

En janvier 2019, le président Donald Trump a manifesté son intention de nommer Keith Krach au poste de sous-secrétaire d'État à la Croissance économique, à l'Énergie et à l'Environnement. Ce dernier devrait être désigné Médiateur permanent. Au moment de la rédaction du présent rapport, la confirmation est pendante au Sénat. Le PFPDT suivra l'évolution de la situation.

2.5 Accès à des données personnelles par des autorités de poursuite pénale

Le PFPDT prend acte du fait que le droit pénal américain limite les droits des ressortissants d'États tiers, lorsque la collecte de données auprès de tiers leur est communiquée après coup. Ces restrictions peuvent avoir des répercussions négatives sur les ressortissants suisses aussi.

III. Conclusion

Le PFPDT se félicite de l'introduction dans le cadre du bouclier de protection des données CH-US des éléments fixés dans l'accord CH-US sur le bouclier de protection pendant la 1re année et de la mise en œuvre des différentes améliorations, demandées par l'UE avant et pendant le 1er examen, qui ont également été intégrées dans le cadre du bouclier de protection CH-US. Il s'agit notamment d'adaptations de la procédure de certification, du renforcement des contrôles menés d'office par les autorités américaines et de la publication de différents documents utiles. Il se réjouit également de la nomination de deux membres du PCLOB, dont le quorum est désormais atteint.

La nomination des cinq arbitres suisses, avant le 1er examen, est également positive. Ces arbitres compléteront la liste des arbitres de l'UE.

Quelques améliorations demeurent néanmoins nécessaires.

Il serait par exemple souhaitable que les autorités américaines étoffent leurs contrôles des entreprises certifiées au titre du bouclier de protection des données.

En outre, la suite des discussions entre la Commission européenne et les autorités américaines sur la définition des données RH aura sans doute un impact sur les employés en Suisse.

S'agissant l'accès aux données personnelles par les autorités américaines, il importe, comme l'a souligné le CEPD dans son rapport du 22 janvier 2019, que le PCLOB, en qualité d'organe de surveillance, publie d'autres rapports, notamment sur les mesures de protection au titre de la PPD 28, de la section 702 FISA et de l'EO 12333.

Au surplus, un Médiateur permanent doit être désigné.

Le CEPD renvoie en outre renvoie en outre aux procédures pendantes devant la CJUE, concernant notamment les clauses contractuelles types, dont l'issue aura des répercussions indirectes pour la Suisse.