Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice

17 septembre 2021

Rapport sur le US CLOUD Act (loi *Cloud*)

BJ-D-443E3401/32

Rapport sur le US CLOUD Act (loi *Cloud*)

Table des matières

Rapport sur le US CLOUD Act (loi *Cloud*)

1 Mandat

En mars 2018, les USA ont adopté le ***C**larifying **L**awful **O**verseas **U**se of **D**ata Act* (*CLOUD Act)*[1]. Dans le domaine de la prévention, de la détection, des enquêtes et des poursuites de crimes graves (*serious crimes*), il doit permettre aux autorités de poursuite pénale américaines d'accéder aux données des fournisseurs de services de communication (*Communication Service Providers*, CSPs) ayant leur siège aux USA, que ces données soient stockées aux USA ou à l'étranger, p. ex. via des filiales, conférant ainsi à la loi américaine un effet extraterritorial[2]. Dans certaines conditions, le *CLOUD Act* permet aux USA de conclure des accords d'exécution bilatéraux (*executive agreements*) avec d'autres États. Ainsi, les autorités de poursuite pénale de l'État partenaire peuvent envoyer des requêtes directement aux CSPs se trouvant aux USA et réciproquement. Pour cela, l'État partenaire doit accepter que les autorités de poursuite pénale américaines accèdent aux données enregistrées par les CSPs ayant leur siège sur son territoire. C'est surtout cet aspect qui incite à se demander dans quelle mesure la conclusion d'un tel accord avec les USA serait opportun pour la Suisse.

En Suisse, l'Office fédéral de la justice (OFJ) est l'organe central dans le domaine de la coopération pénale internationale[3] . À ce titre, il surveille l'application de la loi sur l'entraide internationale en matière pénale (EIMP)[4] et il est en plus responsable du développement des bases légales dans ce domaine. Il a élaboré le présent rapport suite à l'intervention dans ce contexte de différents acteurs de l'économie privée, des associations professionnelles, de l'administration et des autorités de poursuite pénale. Ce document permettra d'approfondir la discussion avec les parties prenantes publiques et privées en Suisse. À cet effet, il apporte notamment des éclaircissements sur les questions juridiques fondamentales qui se posent en termes de compatibilité entre le *CLOUD Act* et le droit suisse.

2 Introduction

Au vu du phénomène de mondialisation, la coopération pénale internationale joue un rôle de plus en plus important. Avec la digitalisation croissante de tous les aspects de la vie, et dans le présent contexte, la collecte et la transmission de preuves électroniques, cette coopération fait face à des défis de nature très différente :

- Les données sont *volatiles* – l'entraide pénale traditionnelle est souvent trop lente pour garantir leur sécurité en temps opportun et au-delà des frontières nationales ;
- Les données n'ont pas de *marquage territorial* – le *lieu de stockage* doit-il vraiment être déterminant pour l'accès des autorités de poursuite pénale aux données ou bien la question n'est-elle pas plutôt de savoir qui peut y avoir *accès* et depuis quel endroit ? Le problème est encore plus complexe pour les *blockchains* car les données ne sont pas stockées physiquement dans un lieu clairement défini ;
- Les données sont *cryptées* – comment peuvent-elles être décryptées efficacement par les autorités de poursuite pénale dans le trafic international des données ? Existe-t-il des règles internationales ou globales ?

Une chose est sûre : la collecte internationale de preuves électroniques remet en question les fondements de la coopération pénale internationale. Elle bouleverse le sens actuel du principe de territorialité. Les procédures d'entraide pénale traditionnelle basée sur la notion de

---

1 Texte complet disponible sur : https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

2 Il faut d'ores et déjà souligner que le *CLOUD Act* s'applique uniquement dans le cadre de *procédures pénales*. Dans ce type de procédure, le principe de territorialité revêt une importance particulière pour diverses raisons. Cf. paragraphes 2. et 5.1 ci-dessous. Par la suite, il sera donc question de *Territorialité au vu du droit pénal*.

3 Cf. art. 17 Loi sur l'entraide pénale internationale (EIMP, RS **351.1**) et art. 3 Ordonnance sur l'entraide pénale internationale (OEIMP, RS **351.11**).

4 RS **351.1.**

souveraineté sont trop lentes. L'accent est mis sur des formes de collaboration plus directes, et parfois sur la participation expresse de particuliers à des procédures pénales à l'étranger. Cela est en partie nécessaire : les capacités des autorités d'entraide judiciaire des États dans lesquels de nombreux CSPs ont leur siège ont atteint leurs limites.

Actuellement, les éventuelles modifications du droit concernant l'entraide judiciaire font l'objet de discussions dans différents forums et au sein de l'UE ainsi qu'au Conseil de l'Europe et à l'ONU.

Grâce à sa proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale d'avril 2018 (règlement *e-evidence*)[5], l'UE souhaite faciliter et accélérer la collaboration entre ses États membres. Au sein du Conseil de l'Europe, le Comité de la Convention sur la cybercriminalité (T-CY), qui représente les États parties à la Convention de Budapest[6], élabore actuellement un deuxième protocole pour cette convention, qui est censé régler de manière générale la collaboration internationale pour les crimes commis au moyen de systèmes informatiques et pour les preuves électroniques. De son côté, l'ONU prépare un instrument multilatéral pour lutter contre la cybercriminalité.

Alors que des instruments multilatéraux censés favoriser la collaboration entre les États font l'objet de discussions dans ces forums, les USA ont, avec le *CLOUD Act,* adopté en mars 2018 au niveau national, une loi dont la portée est extraterritoriale. D'une part, cette loi doit permettre aux autorités de poursuite pénale américaines d'accéder aux données des CSPs dont le siège est aux USA, que ces données soient enregistrées aux USA ou à l'étranger, sans avoir à engager une procédure par la voie de l'entraide judiciaire internationale. D'autre part, elle doit d'autre part permettre aux États étrangers concernés d'avoir également accès aux données des CSPs ayant leur siège aux USA, sans avoir à déposer une requête d'entraide judiciaire, grâce aux accords d'exécution bilatéraux. Il leur suffit pour cela d'envoyer leurs requêtes directement aux CSPs concernés. Cependant, ces États étrangers ne peuvent pas contraindre les CSPs à donner suite à leurs requêtes. L'*executive agreement* permet certes aux CSPs de fournir des données à un État étranger, mais ils n'y sont pas obligés.

La Suisse a conclu un accord d'entraide judiciaire avec les USA dans le cadre du traité du 25 mai 1973 entre la Confédération Suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale ((TEJUS)[7]. Par conséquent, les autorités suisses ont accès aux données des CSPs américains via l'entraide pénale internationale. Cependant, cette procédure est longue car le Département américain de la justice (DOJ) doit examiner la requête correspondante avant de la transmettre à l'autorité d'exécution, qui en général ne peut la satisfaire qu'après une procédure judiciaire, à l'issue de laquelle elle est finalement autorisée à transmettre les moyens de preuve. L'expérience des autorités de poursuite pénale suisses en la matière révèle que les preuves électroniques demandées ne sont pas toujours transmises, ou du moins pas toujours transmises à temps. En 2016, le DOJ a déjà édicté des directives concernant les preuves électroniques afin d'exhorter les autorités étrangères à s'adresser directement aux CSPs, lorsqu'elles souhaitent uniquement avoir accès aux données personnelles des abonnés (*basic subscriber information* : nom et adresse, type et durée du service fourni,

[5] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM/2018/225 final – 2018/0108 (COD) du 17 avril 2018.

[6] Convention du Conseil de l'Europe sur la cybercriminalité, STE 185, RS **0.311.43**.

[7] RS **0.351.933.6.**

moyens de paiement y c. numéros de carte de crédit et de compte ; « données personnelles »)[8] . En pratique, certains CSPs fournissent déjà ce type de données tandis que d'autres refusent de le faire et renvoient à la procédure officielle.

Même si la Suisse concluait un *executive agreement* avec les USA, la situation demeurerait inchangée. En outre, la mise en œuvre de mesures de contrainte ne pourrait être demandée que par la voie de l'entraide judiciaire et cette contrainte pourrait être exercée uniquement par l'intermédiaire de l'autre État. Après la conclusion d'un *executive agreement*, les autorités de poursuite pénale suisses pourraient s'adresser directement à un CSP, également pour des données encore plus sensibles que les données personnelles, mais elles ne seraient pas autorisées à ordonner la mise en œuvre de mesures de contrainte. Si un CSP refusait de lui donner accès à des données, la Suisse devrait engager une procédure d'entraide judiciaire pour les demander et les collecter via des mesures de contrainte. Mais si un CSP acceptait, la collaboration serait plus efficace. Dans ce cas-ci, elle permettrait de délester l'entraide judiciaire avec les USA de sorte que les autorités impliquées pourraient se concentrer sur des cas, pour lesquels les CSPs refusent de coopérer ou qui n'entrent pas dans le champ d'application du *CLOUD Act*. On suppose que les CSPs qui acceptent déjà de coopérer continueront de produire des données personnelles en raison de la clarification de la situation juridique et en s'appuyant sur un *executive agreement*. Les autres CSPs seraient éventuellement intéressés par ce type de collaboration.

3 Le *CLOUD Act*

3.1 Contexte

Le *CLOUD Act* est une loi fédérale américaine qui complète la loi sur les communications enregistrées, le *Stored Communications Act* (SCA), et qui a été promulguée en mars 2018 dans le cadre d'une procédure judiciaire impliquant Microsoft. En 2013, la société Microsoft avait été sommée par un juge américain de communiquer des e-mails et des informations sur un compte hébergé par Microsoft en vertu du SCA. L'entreprise avait communiqué les informations qui se trouvaient sur un serveur hébergé aux USA, mais avait refusé de transmettre les e-mails qui étaient stockés sur un serveur en Irlande. Elle avait argué qu'une entreprise américaine ne pouvait être tenue, sur la base d'une telle injonction, de communiquer des données stockées sur un serveur hébergé à l'étranger. Selon Microsoft, le tribunal américain n'avait aucune compétence en la matière, le SCA n'ayant pas d'effet extraterritorial.

Microsoft a perdu le procès en première instance, mais la Cour d'appel lui a donné raison. Le Département américain de la justice a fait appel de cette décision devant la Cour suprême. Avant même que le jugement ne soit rendu, le Congrès a adopté le *CLOUD Act* qui modifie le SCA et qui confère à la loi son effet extraterritorial actuel.

3.2 Sommaire

3.2.1 Principal contenu matériel

Le *CLOUD Act* oblige les CSPs dont le siège est aux USA et qui gèrent des centres de stockage de données hors des USA, de conserver les données hébergées sur leurs serveurs et de les communiquer sur demande aux autorités judiciaires américaines. Cette loi s'applique in-

[8] Selon la législation actuelle, la demande d'accès aux données personnelles des abonnés doit s'effectuer dans tous les cas par la voie de l'entraide judiciaire.

dépendamment du lieu d'enregistrement de ces données, que ce soit aux USA ou à l'étranger[9]. Sont concernées les sociétés de droit américain, c'est-à-dire celles qui sont soumises à la juridiction américaine[10]. Dans ce cadre, des contacts minimaux (*minimum contacts*) avec les USA sont une condition nécessaire ; l'interprétation et la qualification de ces contacts relèvent toutefois de la compétence des tribunaux américains. Les entreprises détenant des holdings, filiales ou succursales aux USA peuvent également être concernées, tout comme des prestataires étrangers qui font de la publicité pour leurs services de cloud aux USA. Seuls les CSPs étrangers qui n'entretiennent pas ces contacts minimaux avec les USA ne sont pas soumis à de nouvelles obligations.

Le *CLOUD Act* ne stipule aucune durée minimale pour la conservation des données. Toutefois, si l'on se réfère à d'autres dispositions du droit américain, par exemple le SCA, il semble – au moins dans certains cas – qu'une obligation de conserver les données pendant 180 jours s'applique.

En vertu du *CLOUD Act*, le CSP peut contester devant un tribunal américain une injonction des autorités de poursuite pénale concernant la divulgation de données (une motion en modification ou en annulation), si la personne concernée n'est pas une *US person*[11] et si la divulgation des données risque de violer le droit d'un État ayant conclu un *executive agreement* (cf. point 3.2.2 ci-dessous) avec les USA (gouvernement étranger qualifié ou *qualifying foreign government* ; QFG). Pour sa décision concernant l'annulation ou la modification de l'injonction de production des données qui est contestée, le tribunal tient compte des intérêts des USA ou du QFG, des relations entre la personne concernée et, d'une part, les USA et, d'autre part, l'État qui a demandé la divulgation des données, de la probabilité d'une sanction et son éventuelle sévérité, de l'importance des données demandées pour l'enquête, des intérêts des autorités requérantes ainsi que de la probabilité d'accéder opportunément et efficacement aux données correspondantes via des possibilités moins radicales[12]. Si le tribunal le juge nécessaire, la divulgation immédiate des données peut être ordonnée avant même que la décision portant sur une motion en modification ou en annulation n'ait été prise[13].

Ni l'État étranger, ni la personne concernée ne peuvent s'opposer à la requête des autorités américaines. Seul le CSP est en mesure de le faire.

3.2.2 Conclusion possible d'*executive agreements* avec d'autres États sur la base du *CLOUD Act*

3.2.2.1 Généralités

La deuxième partie du *CLOUD Act* permet aux USA de conclure dans certaines conditions des *executive agreements* avec d'autres États. En vertu de ces accords bilatéraux, les autorités compétentes des deux États peuvent demander directement aux CSPs, dont le siège se trouve dans l'un ou l'autre État partie à l'accord, de leur divulguer des informations ou des données stockées sur leurs serveurs. Sur la base d'*executive agreements*, les CSPs peuvent donner directement suite à l'injonction de production internationale (*international production order*, « injonction de production ») envoyée directement par l'autre État. Comme indiqué, les

[9] *CLOUD Act,* §2713. Cf. également BISMUTH, p. 683.

[10] DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 6 ss

[11] *CLOUD Act*, § 2713 (h) (2) (A)

[12] *CLOUD Act*, § 2713 (h) (3) (A)

[13] *CLOUD Act,* § 2713 (h) (4)

CSPs ne peuvent être contraints par l'État étranger de divulguer des données. Une injonction de production ne se substitue donc pas à l'entraide judiciaire, tout du moins lorsque le CSP ne coopère pas de manière volontaire.

3.2.2.2 Conditions matérielles

Selon le *CLOUD Act,* l'État qui souhaite négocier un *executive agreement* avec les USA doit remplir certaines conditions minimales[14] :

La législation nationale de l'État concerné doit offrir de « solides » garanties matérielles et procédurales, comparables à celles des USA, pour protéger la sphère privée et les libertés civiles eu égard à la collecte des données et à ses activités entrant dans le cadre des *executive agreements.* Il doit en effet garantir des dispositions légales adaptées en matière de cybercriminalité et de preuves électroniques. L'État concerné peut notamment en apporter la preuve en faisant valoir son adhésion à la Convention de Budapest.

De manière générale, l'État concerné doit veiller au respect de l'État de droit et du principe de non-discrimination. Il doit en outre se conformer aux obligations internationales en vigueur en matière de droits humains, parmi lesquelles la protection contre les immixtions arbitraires et illégales dans la sphère privée, le droit à une procédure équitable et à la liberté d'expression, d'association et de réunion, l'interdiction des arrestations et détentions arbitraires ainsi que de la torture et des traitements cruels, inhumains ou dégradants.

Les services gouvernementaux qui sont en droit de demander la divulgation de données en vertu des *executive agreements* doivent avoir un mandat clairement défini sur le plan juridique. Ils doivent en outre disposer de directives et de procédures claires concernant la collecte, l'enregistrement, l'utilisation et la divulgation des données. Des mécanismes suffisants, avec lesquels le gouvernement étranger peut prouver la transparence concernant la collecte et la saisie de données électroniques, doivent être disponibles.

L'État concerné doit apporter la preuve qu'il s'efforce d'encourager et de protéger la libre circulation de l'information dans le monde et de promouvoir le caractère ouvert, libre et interconnecté de l'Internet[15]. Enfin, il doit garantir des droits réciproques pour l'accès aux données. Cela signifie qu'il doit autoriser les CSPs siégeant sur son territoire à répondre directement aux requêtes des autorités de poursuite pénale américaines.

Une injonction de production reposant sur l'*executive agreement* ne doit pas viser directement des citoyens américains ou *US persons.* L'État concerné doit donc prendre des mesures appropriées pour éviter une telle situation. Le *CLOUD Act* contient la liste complète des autres conditions que doit remplir une injonction de production[16].

3.2.2.3 Conditions formelles

Aux USA, la conclusion des *executive agreements* relève des compétences de l'exécutif. Le procureur général des USA (US Attorney General) décide avec le Ministre des Affaires étrangères si l'autre État remplit les conditions nécessaires à la conclusion de l'accord bilatéral et transmet la confirmation écrite au Congrès américain[17]. L'*executive agreement* certifié de

[14] *CLOUD Act,* § 2523 (b)

[15] *CLOUD Act*, §2523 (b) (1) (B) (vi)

[16] *CLOUD Act,* § 2523 (b) (2) et (3)

[17] *CLOUD Act,* §2523 (b)

la sorte peut entrer en vigueur aux USA si le Congrès ne formule pas de recours dans un délai de 180 jours[18].

L'accord est conclu pour une durée déterminée. L'État qui conclut un tel accord avec les USA doit dès lors se soumettre à une évaluation périodique par les autorités américaines[19].

3.2.3 Contenu de l'accord bilatéral

La première partie de l'*executive agreement* doit contenir des dispositions à caractère général telles que des définitions, le droit applicable, la forme et le contenu des requêtes, les autorités compétentes et des dispositions relatives à la protection des données.

L'une des principales définitions est celle du *serious crime* (infraction grave). En vertu du *CLOUD Act,* les requêtes fondées sur un *executive agreement* doivent se limiter aux enquêtes pénales portant sur des infractions graves. Outre les actes de terrorisme, explicitement mentionnés dans le *CLOUD Act*, ces infractions concernent notamment les meurtres et les enlèvements d'enfants. Il convient aussi de déterminer les données pouvant être prises en compte dans l'*executive agreement,* à savoir exclusivement les données déjà enregistrées ou également les données collectées en temps réel. Le concept de CSP, avec ce qu'il englobe précisément, doit également être défini.

En Suisse, la collaboration en matière d'entraide judiciaire se heurte à différentes limites. Si l'on considère que le *CLOUD Act* permet une forme de collaboration internationale dans des affaires pénales, il serait judicieux de vérifier, dans le cas de la négociation éventuelle d'un *executive agreement,* dans quelle mesure les principes essentiels du droit suisse sont intégrés dans le texte en vue d'une collaboration. Les éventuels motifs d'irrecevabilité devraient y être négociés et intégrés de manière explicite.

Par conséquent, un éventuel *executive agreement* doit également comporter des dispositions techniques relatives à la transmission d'informations et à l'enregistrement de données. L'accord doit stipuler que la transmission des données et des informations doit se faire via un canal sûr. Il doit également préciser les exigences relatives à l'enregistrement de données dans un système sécurisé et à l'accès à ces données dans l'État requérant.

Sur le plan formel, l'*executive agreement* doit comporter des dispositions concernant les procédures à respecter, notamment sur la question des objections ou des motions en annulation portant sur des injonctions de production.

3.2.4 Conditions requises pour les injonctions de production en vertu d'un *executive agreement*

Conformément au *CLOUD Act,* les injonctions de production fondées sur un *executive agreement* doivent remplir différentes conditions minimales[20].

La personne dont les données sont concernées par une injonction de production émanant de l'étranger ne doit pas être une *US person*, c'est-à dire qu'elle ne doit ni être citoyenne américaine, ni résider aux USA. Dans le cas d'une entreprise, elle ne doit pas avoir son siège aux USA[21]. À l'inverse, les autorités de poursuite pénale américaines n'auraient pas le droit

[18] *CLOUD Act*, §2523(d) (2)

[19] *CLOUD Act,* §2523(b) (4) (J)

[20] *CLOUD Act*, § 2523 (b) (3)

[21] Selon *CLOUD Act*, § 2523 (a) (2) « incorporated in the United States ».

d'exiger la divulgation de données de personnes de nationalité suisse, de personnes résidant en Suisse ou d'une société dont le siège est en Suisse, pour autant que ce point soit précisé dans l'accord. Dans le cadre de l'*executive agreement,* l'État étranger n'a pas le droit d'envoyer des injonctions qui visent directement une *US person* ni d'ailleurs des injonctions qui concernent certes une *non US person,* mais qui ont pour but de collecter des informations sur une *US person* et inversement[22]. Le traitement qui serait réservé aux filiales d'entreprises suisses fondées selon le droit américain n'est pas clair dans ce contexte. Lorsqu'il s'agit de personnes qui sont exclues du domaine d'application de l'*executive agreement*, il convient de demander les données correspondantes dans le cadre de l'entraide judiciaire.

L'injonction de production doit concerner un *serious crime*, une notion à définir dans l'*executive agreement* (cf. point 5.3). En outre, en conformité avec la législation de l'État à l'origine de l'injonction, elle doit indiquer une personne, une adresse, un objet personnel ou une autre caractéristique d'identification et être justifiée par des faits compréhensibles et crédibles (pas de *fishing expeditions*). En outre, elle doit pouvoir être vérifiée par un tribunal ou une autorité indépendante et dans le cas des injonctions de mise sur écoute, elle doit être limitée dans le temps et proportionnelle[23].

L'injonction ne doit pas apporter la preuve qu'il existe une *probable cause*[24], ce qui faciliterait la collaboration avec les USA et délesterait considérablement les autorités de poursuite pénale suisses.

4 Droit comparé

4.1 *Executive agreement* entre les USA et le Royaume-Uni

Le Royaume-Uni (RU) est le premier, et à ce jour le seul État avec lequel les USA ont négocié un *executive agreement* en vertu du *CLOUD Act*. Le contenu précis de l'accord signé le 3 octobre 2019, mais qui n'est pas encore entré en vigueur, est disponible en ligne[25], Ce premier accord revêt une importance particulière car il devrait également définir les grandes lignes des futurs *executive agreements*.

Il s'agit d'un accord relativement court dont plusieurs des points renvoient à d'autres accords, à savoir la Convention de Budapest, l'accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel[26] et l'accord d'entraide judiciaire en matière pénale conclu entre les USA et le Royaume-Uni. De par sa structure, cet accord est comparable à un accord d'entraide judiciaire en matière pénale. Il contient des définitions, une finalité, des limites, des dispositions sur la protection des données, etc.

Parmi les notions importantes définies dans le cadre de l'*executive agreement* figurent notamment les autorités compétentes, le CSP, les données et le *serious crime* (Art. 1). Les injonctions de divulgation ou de production de données enregistrées hors de l'État (« injonction ») doivent être conformes au droit national de la partie requérante (art. 5, al. 1). En revanche, le droit national de la partie dans laquelle se trouve le CSP ne doit pas forcément être respecté. L'injonction doit pouvoir être portée devant une autorité judiciaire ou une

[22] *CLOUD Act,* § 2523 (b) (3) (A) et (B)

[23] *CLOUD Act,* § 2523 (b) (3) (D)

[24] DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 8.

[25] Contenu disponible sur : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. D'après les informations de l'Ambassade britannique à Berne, l'accord devrait entrer en vigueur à la fin de l'été 2021.

[26] Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, JO L 336 du 10 décembre 2016, p. 3.

autorité indépendante de la partie requérante afin que ces autorités puissent vérifier que l'injonction est compatible avec la législation nationale (art. 5, al. 2). Cela signifie qu'un CSP dont le siège est aux USA et qui reçoit une injonction du Royaume-Uni peut porter l'affaire devant les autorités britanniques. Pour les petits CSPs, il peut s'avérer difficile d'intenter une action en justice dans un autre pays, en particulier aux USA. L'*executive agreement* prévoit donc une sorte d'autorité centrale qui doit contrôler la conformité de l'injonction avec l'accord, avant qu'elle ne soit envoyée au CSP (Art. 5, al. 6). Selon cette disposition, une autorité souhaitant collecter des informations auprès d'un CSP doit d'abord consulter cette autorité centrale.

Si un CSP considère que l'injonction reçue n'est pas conforme à l'accord, il doit d'abord l'invoquer auprès des autorités désignées de l'État qui transmet l'injonction, soit l'État dans lequel il n'est pas incorporé. En cas de désaccord subsistant, il peut alors également s'adresser aux autorités désignées dans l'État dans lequel il est incorporé (art. 5, al. 11). Les deux autorités s'efforcent de trouver une solution consensuelle. Si l'État « requis » considère que l'injonction n'est pas conforme à l'accord, il peut en informer l'autorité de la partie « requérante » et l'accord ne sera pas applicable à l'injonction (art. 5, al. 12). Il semblerait donc qu'il y ait une procédure selon laquelle l'autorité centrale de l'État de résidence peut décider en dernière instance si une injonction est conforme ou non à l'*executive agreement.*

Les données obtenues sur la base de l'accord ne peuvent être transmises à un État tiers sans le consentement de l'État dans lequel le CSP est incorporé (Art. 8, al. 2). Si la personne dont les informations sont demandées ne se trouve pas sur le territoire de l'État « requérant » et si elle n'est pas citoyenne de cet État, l'État tiers dont elle est ressortissante doit en être informé[27].

Si les données concernent des cas qui pourraient mener à la prononciation d'une peine de mort aux USA ou à la violation de la liberté d'expression au Royaume-Uni, l'autorité centrale de l'autre État doit être impliquée et donner son accord (art. 8, al. 4). Sans l'accord de l'autre État, les données obtenues sur la base du *CLOUD Act* au Royaume-Uni ne peuvent être utilisées pour prononcer une peine de mort aux USA et les données obtenues aux USA ne peuvent servir à prononcer une sanction liée à une violation de la liberté d'expression au Royaume-Uni[28]. Il existe donc des droits de véto correspondants[29].

En ce qui concerne les personnes visées par l'*executive agreement*, il y a une asymétrie entre les USA et le Royaume-Uni. En effet, les injonctions britanniques ne peuvent pas viser des *US persons.* Cela inclut à la fois les personnes qui résident aux USA, quelle que soit leur nationalité, et les citoyens américains qui résident à l'étranger. À l'inverse, les injonctions américaines peuvent en principe viser des citoyens britanniques. Les personnes qui ne sont pas de nationalité anglaise, mais qui résident *sur le territoire britannique* sont exclues du champ d'application de l'accord. Cette disposition semble s'appuyer sur les principes du droit de l'UE (citoyenneté européenne)[30].

Dans le cadre de l'*executive agreement,* les CSPs ne sont pas tenus de se conformer aux requêtes provenant des autorités de l'autre État. Si un CSP refuse de répondre, c'est la loi

---

27 DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ». Art. 5 de l'accord.

28 CHRISTAKIS, « 21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement », pt. 15–16 ; Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 19–20.

29 DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ».

30 Contenu disponible sur : https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement.

du pays qui émet la requête qui s'applique[31]. Si une mesure de contrainte est nécessaire, il faudra en principe passer par la voie de l'entraide pénale internationale. L'accord est neutre en ce qui concerne le cryptage. Il n'oblige pas les CSPs à supprimer les cryptages[32].

Les parties évaluent le respect de l'*executive agreement* un an après son entrée en vigueur, puis de manière périodique (art. 12, al. 1). Chaque partie doit également établir un rapport annuel sur l'application de l'accord qu'elle soumettra à l'autre État (art. 12, al. 4). L'accord s'applique pendant une durée de cinq ans et pourra par la suite être résilié ou prolongé pour une durée indéterminée.

4.2 Législation *e-evidence* de l'UE et US *CLOUD Act* : conflit ou négociation ?

4.2.1 Législation *e-evidence* de l'UE

Des efforts sont actuellement entrepris au niveau de l'UE pour améliorer l'accès transfrontalier aux preuves électroniques (dites *e-evidence*). Un cadre juridique visant à faciliter et à accélérer la sécurisation des preuves électroniques et leur accès transfrontière pour les autorités policières et judiciaires est en cours d'élaboration. L'idée d'une législation sur les preuves électroniques remonte aux attaques terroristes de mars 2016 à Bruxelles et à la demande qui en a résulté dans l'UE de trouver de nouveaux moyens de sécuriser les preuves électroniques plus rapidement et plus efficacement et de coopérer plus étroitement avec les pays tiers et les prestataires de services opérant sur le territoire européen[33].

En avril 2018, la Commission a présenté deux propositions législatives sur les *e-evidence*, à savoir : une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[34] et une proposition de directive établissant des règles communes relatives à la désignation de représentants légaux aux fins de la collecte de preuves dans le cadre de procédures pénales[35].

La proposition de règlement introduit deux nouveaux instruments contraignants pour les autorités concernées, à savoir l'injonction européenne de production (EPOC) et l'injonction européenne de conservation (EPOC-PR). Ces instruments doivent exister en parallèle des instruments juridiques actuels qui facilitent la collecte de preuves sur le territoire d'un autre État membre, tels que la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale (« directive décision d'enquête européenne »)[36].

L'injonction européenne de production doit permettre aux autorités d'utiliser une ordonnance judiciaire pour demander des données numériques stockées par un CSP dans un autre État membre de l'UE et nécessaires comme preuve dans le cadre d'enquêtes et de procédures pénales. Cette idée repose essentiellement sur le fait que chaque CSP souhaitant fournir des services dans l'UE doit désigner un représentant dans l'UE (appelé *legal representative*)

---

[31] Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 18.

[32] CHRISTAKIS, « 21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement », pt. 14 ; DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ».

[33] Déclaration commune des ministres européens de la justice et de l'intérieur et des représentants des institutions de l'UE du 24 mars 2016 sur les attentats terroristes perpétrés le 22 mars 2016 à Bruxelles, disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/.

[34] Proposition de la Commission européenne pour un règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale du 17 avril 2018, COM (2018)225 final.

[35] Proposition de la Commission européenne pour une directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale du 17 avril 2019, COM(2018) 226 final.

[36] Directive 2014/41/EU du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, JO L 130 du 1er mai 2014, p. 1.

qui a accès aux données de l'ensemble de l'entreprise. La proposition de directive prévoit des règles uniformes pour la désignation de ces représentants. Les autorités (police ou ministère public d'un État membre de l'UE) peuvent ainsi avoir un accès direct à ce représentant pour la notification et l'exécution des injonctions – quel que soit le lieu où ce représentant a son siège dans l'UE. Ici également, le contact n'a donc plus lieu entre les autorités d'un État, mais entre une autorité et une entreprise, c'est-à-dire une entité privée[37]. Les entreprises concernées doivent transmettre les données dans un délai de quelques jours à quelques heures (10 jours, en cas d'urgence dans les 6 heures).

L'injonction européenne de conservation – tout comme l'injonction européenne de production – est adressée au représentant d'un CSP qui se trouve en dehors du système juridique de l'État membre émetteur de l'injonction. Avec l'injonction de conservation, les CSPs peuvent être contraints de sauvegarder les données en vue d'une demande ultérieure de remise[38].

L'affaire est actuellement discutée en trilogue, terme qui désigne le processus de coordination politique entre la Commission européenne, le Conseil de l'UE et le Parlement européen.

4.2.2 Discussions entre l'Union européenne et les USA

En février 2019, la Commission européenne a sollicité un mandat pour l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale[39]. En juin 2019, le Conseil de l'Union européenne a autorisé la Commission à entamer des négociations au nom de l'UE[40].

L'ouverture de discussions avec les USA s'explique principalement par la législation de l'UE sur les preuves électroniques. Bien que les propositions relatives aux preuves électroniques concernent les CSPs qui fournissent des services sur le marché de l'UE, il y a un risque de conflit entre les obligations prévues dans ces propositions et les dispositions légales d'États tiers. Certes, les projets concernant la législation sur les preuves électroniques de l'UE contiennent des dispositions régissant les conflits de lois. Cependant, étant donné que les principaux CSPs visés dans les procédures pénales au sein de l'UE ont leur siège aux USA et qu'ils sont donc placés sous la souveraineté américaine, un accord entre l'UE et les USA doit permettre d'éviter d'éventuels conflits d'obligations entre les deux systèmes. L'objectif de l'UE est d'éviter, avec un accord international, des conflits de lois, notamment sur le plan des données relatives au contenu, et d'accélérer l'accès aux preuves électroniques. Étant donné que le droit américain en vigueur interdit aux CSPs américains de répondre aux requêtes d'autorités de poursuite pénale étrangères portant sur des données liées au contenu et que les autorités judiciaires et de poursuite pénale de l'UE rencontrent actuellement des difficultés pour collecter ces données au moyen de requêtes d'entraide pénale, un accord doit offrir un cadre juridique suffisant à ces autorités et permettre une collaboration directe avec les CSPs. Ainsi, du point de vue de l'UE, un accord entre l'UE et les USA permettrait avant tout de compléter l'objectif et l'efficacité des propositions sur les preuves électroniques, notamment en ce qui concerne les données liées au contenu détenues par un CSP américain basé aux USA.

---

37 TSILIKIS, p. 169 ss et 172 ss

38 Pour un aperçu complet, voir les explications dans la proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, consid. 47.

39 Recommandation de la Commission européenne du 5 février 2019 pour une décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les USA sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.

40 Contenu disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

Concernant les données non liées au contenu, les autorités américaines invitent dès à présent les autorités de poursuite pénale et judiciaire de l'UE à s'adresser directement aux CSPs américains, si elles souhaitent collecter ces données compte tenu du nombre croissant de requêtes d'entraide pénale (voir l'introduction). À cet égard, le droit américain autorise les CSPs dont le siège est aux USA de donner suite à ces requêtes, sans toutefois les y contraindre. Un accord entre l'UE et les USA doit par conséquent améliorer la sécurité juridique également en ce qui concerne l'accès à des données non liées au contenu détenues par un CSP américain[41].

Selon des contacts informelles, les négociations entre l'UE et les USA ne constituent pas des négociations « CLOUD-Act » à proprement parler. Leur objectif est plutôt d'établir une passerelle entre le *CLOUD Act* américain et la législation de l'UE sur les preuves électroniques. Tandis que, dans le cadre de ce processus, l'UE tente d'imposer son système de preuves électroniques, les USA souhaitent favoriser l'établissement du *CLOUD Act.* Deux approches exactement opposées ayant été choisies pour ces deux systèmes (USA : effet extraterritorial ; UE : obligation du CSP et/ou du représentant d'avoir une présence « territoriale »), ils ne sont donc pas pleinement compatibles. L'objectif est toutefois de pouvoir s'adresser directement aux CSPs des deux côtés de l'Atlantique, quel que soit le continent où leur siège est établi. En vertu de l'accord, les aspects juridiques relatifs à l'accès aux données liées ou non liées au contenu qui sont en possession des CSPs en Europe et aux USA, doivent être soumis aux mêmes prescriptions.

D'après des sources informelles, quatre séances de négociations ont eu lieu jusqu'à présent. La protection des données a occupé une place essentielle dans les discussions. Sur ce point, la Commission a déclaré que l'accord-cadre entre l'UE et les USA sur la protection des données devait être complété.[42] D'importantes divergences subsistent encore sur de nombreux points. Cependant, il ne devrait pas être aisé pour la Commission d'avancer de manière substantielle dans les discussions, tant que les négociations en trilogue sur les preuves électroniques ne sont pas terminées. En effet, sa position dans les négociations dépend en grande partie de l'issue de cette procédure[43]. La forme de l'accord reste à définir. Il devra en outre s'insérer dans le cadre juridique actuel[44], et les rapports entre ces différentes sources juridiques devront être clarifiés.

Les négociations avec les USA seront également influencées par les négociations menées parallèlement au sein du Conseil de l'Europe à propos d'un deuxième protocole additionnel à la Convention du Budapest. Ces dernières porteront sur des questions similaires et entraîneront des difficultés comparables car l'UE a une grande influence dans les négociations relatives à ce protocole (cf. point 4.3). Le contenu de ce protocole peut donc avoir des répercussions directes sur les négociations entre l'Union européenne et les USA[45].

---

41 Recommandation du 5 février 2019 pour une décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les USA sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.

42 Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, JO L 336, 10.12.2016, p. 3–13).

43 Report of the Commission services on the second round of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 6 novembre 2019, disponible sur : https://www.statewatch.org/news/2019/nov/eu-council-usa-E-Evidence-13713-19.pdf.

44 Cf. p. ex. l'accord entre l'Union européenne et les USA en matière d'entraide judiciaire ainsi que la Convention de Budapest et les conventions bilatérales avec les États membres.

45 Fiche d'information de la Commission européenne du 5 février 2019, questions et réponses : Mandat en vue du deuxième protocole additionnel à la convention de Budapest disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_19_865 (actualisé le 1.7.2020).

Une fois l'accord négocié, le Parlement européen doit encore approuver le texte de l'accord et le Conseil doit statuer sur la conclusion de l'accord.

4.3 Deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention du Budapest)[46]

Le deuxième protocole additionnel à la Convention de Budapest qui est actuellement élaboré au sein du Conseil de l'Europe poursuit le même objectif de base que les instruments et procédures déjà mentionnés. Cet instrument doit lui aussi permettre aux autorités de poursuite pénale d'accéder plus facilement aux preuves électroniques. Il doit optimiser et accélérer la collaboration future entre les États contractants – parmi lesquels les USA – dans lesquels les principaux CSPs ont leur siège, lors des poursuites contre la *cyber-enabled criminality*. Cet instrument doit en particulier permettre aux autorités de poursuite pénale d'accéder plus facilement aux preuves électroniques, surtout quand ces dernières se trouvent à l'étranger. La collaboration avec les prestataires étrangers doit être facilitée.

Le protocole contient donc des dispositions qui doivent obliger les parties contractantes à créer dans leur législation nationale une réglementation permettant une collaboration directe avec les CSPs sur le territoire d'une autre partie contractante. Cela concerne l'accès à des informations sur les noms de domaine ou des données d'utilisateur, des méthodes garantissant une divulgation plus rapide des informations d'utilisateur, des données de connexion et, en cas d'urgence, des données enregistrées. D'autres dispositions précisent les conditions préalables à la collaboration ainsi que des clauses concernant les motifs d'irrecevabilité, en particulier la protection des données.

Les objectifs poursuivis dans le cadre du deuxième protocole additionnel, qui visent la suppression et la « délocalisation » de garanties fondées sur le droit et les procédures afin d'accélérer la coopération, sont cependant en contradiction avec l'exigence selon laquelle l'accord doit être ratifié dans le monde entier par le plus grand nombre possible d'États. Le Conseil de l'Europe a considérablement abaissé le seuil d'adhésion de pays tiers à la Convention de Budapest. Ainsi, des États qui parfois ne souhaitent pas ou ne sont pas en mesure de garantir les droits humains fondamentaux ni les garanties procédurales sont invités à adhérer à cette convention.

Concrètement, ce protocole peut aboutir à une collaboration simplifiée dans le cadre des poursuites pénales sans pour autant garantir un respect suffisant des garanties procédurales et des droits humains. Dans ce contexte, il est difficile d'imaginer la création d'une « *community of trust among the States Parties »* parfois citée, si le cercle des États contractants ne cesse de s'agrandir et si ces pays ne peuvent ou ne souhaitent pas respecter les garanties procédurales ni les droits fondamentaux, tels qu'ils sont perçus par la Suisse.

Les travaux du Conseil de l'Europe auraient dû être terminés en décembre 2020, mais cela n'a pas été possible en raison des divergences parfois importantes entre les délégations (points de vue divergents exprimés par la délégation américaine et divergences entre l'Australie, le Canada, le Japon d'une part et l'Union européenne d'autre part). Compte tenu du dilemme décrit ici entre d'une part l'universalisation du protocole et la simplification de la coopération et, d'autre part, les aspects en lien avec la protection juridique, on peut se demander si la Suisse cherchera à obtenir une signature rapide du protocole. À l'heure actuelle, une

[46] Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest), STE 185, RS **0.311.43** ; https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185.

procédure prudente, avec une analyse régulière des expériences et des répercussions à court et moyen terme, semble judicieuse.

Il convient d'ajouter que des travaux préparatoires en vue de la mise en place d'une convention mondiale sur la cybercriminalité ont débuté au niveau mondial sous l'égide de l'ONU. Il va de soi que les divergences mises en évidence par les discussions autour du deuxième protocole de la Convention de Budapest se manifestent ici avec une acuité encore plus forte. Ces travaux ne sont toutefois pas suffisamment avancés à l'heure actuelle ; c'est pourquoi, le présent rapport ne les aborde pas en détail.

5 Les questions juridiques

5.1 Territorialité et souveraineté

Le principe de territorialité est un pilier central du droit international, notamment en ce qui concerne les questions de délimitation dans le domaine de la compétence pénale. Il est étroitement lié à la souveraineté des États. En termes positifs, celle-ci comprend la compétence des États à s'organiser juridiquement et structurellement ainsi qu'à conclure des traités internationaux, et en termes négatifs, l'interdiction de s'immiscer dans les affaires intérieures d'autres États (interdiction d'intervention[47]). L'interdiction pour les États de porter atteinte à la souveraineté et à l'intégrité territoriale d'autres États par leur législation ou leurs actions concrètes découle du principe de territorialité et des limites fixées par l'obligation de non-ingérence des États.

Dans l'*arrêt Lotus*[48] de 1927, qui reposait sur un incident en haute mer impliquant la France et la Turquie, la Cour Permanente de Justice Internationale (CPJI) a estimé que le principe de territorialité n'exclut pas des applications du droit au-delà de son propre territoire, tout du moins si celles-ci ne sont pas explicitement interdites par le droit international. Dans un arrêt de 1992, le Tribunal fédéral y fait également référence : « [L']application extraterritoriale de son propre droit [n'est] *a priori* pas non plus considérée comme inadmissible en droit international et en droit pénal international [...]. Au contraire, selon la doctrine et la pratique dominantes, la législation nationale peut également s'appliquer à des faits extraterritoriaux s'il existe une relation interne univoque entre ces faits et le droit national »[49].

Le commerce international, la mobilité mondiale et, en particulier, la communication moderne avec des données disponibles à l'échelle mondiale et accessibles à tout moment ne remettent pas fondamentalement en cause le principe de territorialité. Cependant, ils multiplient les points de contact et les risques de collision entre les différents ordres juridiques des États. Il est donc d'autant plus important de tracer des limites claires entre les applications de la loi hors du territoire de l'État, autorisées par le droit international, et les dépassements interdits de la compétence extraterritoriale. Les points de rattachement reconnus en droit international sont notamment le rattachement territorial (p. ex. la résidence ou le domicile d'une personne, le siège ou la succursale d'une société, le lieu d'exercice d'une activité) ou le rattachement personnel (p. ex. la nationalité de l'auteur ou de la victime d'un acte). Dans certains cas particuliers, pour préserver par exemple sa propre sécurité en cas d'attaques ou de menaces graves ou des intérêts fondamentaux généralement reconnus de la communauté internatio-

47 Art. 2, al. 7 Charte des Nations Unies, RS **0.120**.

48 Publications de la Cour Permanente de Justice Internationale (CPJI), Recueil des Arrêts, Série A – n° 10, p. 18 ss, arrêt n° 9 : Affaire du « Lotus » du 7 septembre 1927.

49 ATF 118 Ia 137 consid. 2b p. 142, traduit de l'allemand.

nale, comme la lutte contre les crimes les plus graves dans le cadre du principe d'universalité, un rattachement à un comportement matériel spécifique peut également être suffisant.

Le droit pénal reprend également ces principes de droit international[50]. Cependant, en tant que dernier et plus radical moyen dont dispose un ordre démocratique pour défendre ses valeurs[51], le lien avec la souveraineté et la territorialité est particulièrement étroit en droit pénal. Contrairement aux procédures civiles, les procédures pénales n'impliquent jamais la collaboration des parties – et surtout pas de la personne accusée. Au contraire, celle-ci peut revendiquer le principe selon lequel elle ne doit pas s'incriminer elle-même[52]. La collecte de preuves dans le droit de la procédure pénale inquisitoire des États d'Europe continentale est donc fondamentalement une tâche étatique. L'*État* établit, du moins selon la fiction, la vérité[53]. La collecte des preuves en droit pénal est donc associée à des possibilités d'accès direct pour les autorités de poursuite pénale. En raison du rôle central des organes de l'État dans la collecte des preuves en droit pénal, l'État *sur le territoire duquel se trouvent les preuves* est fondamentalement responsable de sa réalisation. Le lieu d'un bien joue donc un rôle central dans la procédure pénale : l'autorité de poursuite pénale compétente sur le lieu de stockage est généralement responsable de la collecte des preuves matérielles. Jusqu'à présent, ce principe a également été transposé aux données qui doivent aussi être collectées sur le « lieu de stockage ».

Le *CLOUD Act* n'adhère à ces principes que dans une certaine mesure. Son champ d'application est très large en termes d'espace, de temps et de contenu (cf. point 3.2). Tous les CSPs basés aux USA sont couverts par la loi. Ainsi, la loi s'applique aux données stockées ou contrôlées par des CSPs étrangers en dehors des USA, si ces CSPs exploitent des succursales commerciales aux USA. Même des fournisseurs étrangers de services destinés au marché américain, qui résideraient à l'étranger, pourraient être concernés[54]. D'une part, les autorités de poursuite pénale américaines peuvent sur la base du *CLOUD Act* collecter des données qui ne sont pas stockées aux USA. D'autre part, elles peuvent s'adresser à des entreprises qui ne sont pas basées aux USA et ne sont donc pas nécessairement soumises à leur juridiction. Ce deuxième cas de figure peut être considéré comme problématique au regard de la territorialité. Selon le *CLOUD Act*, les autorités américaines peuvent s'adresser directement à une personne privée (le CSP) sur le territoire de l'autre État, sans que celui-ci en soit informé. En outre, le CSP étranger ne dispose que de procédures américaines qui lui sont inconnues pour engager un recours, de sorte qu'il pourrait être désavantagé.

Même si cela ne remet pas fondamentalement en question le principe de territorialité en droit international, le champ d'application du *CLOUD Act* peut entraîner des *conflits de compétence extraterritoriale en droit pénal*. La question de la « tolérance » d'un tel accès extraterritorial aux données devrait être réglée dans un éventuel *executive agreement.*

5.2 Nature des *executive agreements*

Le *CLOUD Act* prévoit que les USA peuvent conclure des *executive agreements* avec d'autres États (cf. point 3.2.2). Sur la base de ces accords, les autorités de poursuite pénale de pays dotés d'un système constitutionnel démocratique (du point de vue des USA), de

[50] Voir à cet égard les principes de territorialité, de personnalité et du droit international sur lesquels la compétence pénale s'appuie.

[51] Cf. FRANZ RIKLIN, *Schweizerisches Strafrecht, Allgemeiner Teil I, Verbrechenslehre*, Zurich 2007, §4 N 7.

[52] Cf. art. 6, al. 1 CEDH et art. 113, al. 1, art. 140, art. 158, al. 1, let. b, art. 262, al. 2 et art. 265, al. 2, let. a CPP.

[53] Cf. art. 2 et art. 6 CPP.

[54] Voir le rapport à l'intention de l'Assemblée nationale française « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » du 26 juin 2019, point 1.2.4.2.1, p. 29 ss ; disponible sur : https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf.

standards de protection des données et de garanties procédurales comparables à celles des USA doivent pouvoir contacter directement les CSPs aux USA, afin de collecter des données pour la poursuite de *serious crimes*. Dans le même temps, ces États partenaires tolèrent l'accès des autorités de poursuite pénale américaines aux données des CSPs situés sur leur territoire. Le cas échéant, les données sont communiquées directement entre le CSP et l'État « requérant » respectif, sans procédure d'entraide judiciaire.

Le *CLOUD Act per se (*c'est-à-dire même sans *executive agreement* additionnel*)* offre aux autorités de poursuite pénale américaines, comme cela a été expliqué, la possibilité d'obtenir l'accès à des données détenues et stockées par un CSP américain n'importe où dans le monde dans le cadre d'une procédure pénale engagée par l'administration américaine. Dans ce contexte, la possibilité de conclure des *executive agreements* avec d'autres États sous certaines conditions est un élément important pour promouvoir l'acceptation du *CLOUD Act*. Ce faisant, les USA s'appuient sur l'attractivité de leur pays dans le domaine de la fourniture de services de communication et offrent la réciprocité à leurs partenaires, afin de combler la lacune du *CLOUD Ac*t en matière de respect du principe de territorialité en droit international. Le manque de protection juridique est également abordé : si une procédure est ouverte aux USA contre un ressortissant étranger, les autorités américaines peuvent en principe demander la divulgation de ses données sur la base du *CLOUD Act.* Toutefois, il existe une exception concernant la divulgation des données d'un ressortissant étranger d'un pays avec lequel les USA ont conclu un *executive agreement*. Si un tel accord existe, les CSPs peuvent intenter une motion en modification ou en annulation en vertu du *CLOUD Act,* si leur client n'est pas une *US person* et si la divulgation des données risque de violer la loi du QFG. Un *executive agreement* pourrait donc offrir une certaine protection aux ressortissants suisses et aux personnes soumises à la juridiction suisse. Si la divulgation risque d'enfreindre la législation suisse, les CSPs pourraient engager une action en justice aux USA pour protéger les droits des personnes concernées. En conséquence, un *executive agreement* fournirait une certaine protection contre l'accès non autorisé des autorités de poursuite pénale américaines aux données (personnelles) en Suisse. La manière dont cette protection devrait être conçue afin de satisfaire aux exigences du droit suisse de rang supérieur est examinée ci-après aux points 5.5 et 5.6.

D'un point de vue formel, il convient de noter que le *CLOUD Act*, en tant que loi fédérale américaine, décrit lui-même les conditions préalables à la conclusion, le champ d'application matériel et les principaux contenus des *executive agreements*. Néanmoins, d'un point de vue formel, les *executive agreements* sont des traités bilatéraux qui relèvent de la Convention de Vienne sur le droit des traités[55]. Ainsi, ce sont les règles générales du droit international et la pratique développée sur cette base qui s'appliquent à ces traités et à leur interprétation, et non, par exemple, le droit américain ou la jurisprudence américaine. L'application du droit américain ne serait possible que si un *executive agreement* faisait directement référence au droit américain. L'accord conclu entre les USA et le Royaume-Uni n'y fait pas référence[56]. Il contient des obligations et des droits indépendants qui ne découlent pas du droit national. Du point de vue du droit international, les dispositions du *CLOUD Act* traitant des *executive agreements* s'apparentent donc plutôt à des « instructions » du législateur américain à l'adresse de son propre gouvernement.

En Suisse, les traités internationaux doivent être approuvés par l'Assemblée fédérale. Le Conseil fédéral les signe et les soumet à l'approbation de l'Assemblée fédérale. Après un

[55] Convention de Vienne sur le droit des traités du 23 mai 1969, RS **0.111**.

[56] Agreement between the United Kingdom and the USA on Access to Electronic Data for the Purpose of Countering Serious Crime du 3 octobre 2019, note de bas de page 21.

vote favorable, il les ratifie (art. 184, al. 2 de la Constitution fédérale [Cst.][57]). Exceptionnellement, le Conseil fédéral peut conclure des traités de sa propre initiative. C'est le cas si sa compétence découle d'une loi ou d'un traité international (art. 166, al. 2 Cst.). Le cas échéant, l'Assemblée fédérale lui accorde par délégation le pouvoir de conclure des traités. En outre, le Conseil fédéral peut conclure seul des traités internationaux de portée mineure (art. 7a, al. 2 de la loi sur l'organisation du gouvernement et de l'administration [LOGA][58]).

Un *executive agreement,* tel que celui qui est réglé par le *CLOUD Act*, ne serait pas un traité de portée mineure. Comme il permettrait aux autorités suisses et américaines de collecter des données directement auprès des CSPs, il affecterait considérablement le droit de la protection des données et les garanties procédurales des personnes physiques ou morales concernées. En outre, bien que la législation suisse contienne une norme de délégation en faveur du Conseil fédéral dans le domaine de la protection des données (art. 67 nLDP), cette règle ne pourrait pas s'appliquer à un *executive agreement* basé sur le *CLOUD Act*. On peut donc supposer que l'approbation de l'Assemblée fédérale serait requise conformément à l'art. 184, al. 2 de la Constitution fédérale.

La conclusion d'un *executive agreement* aurait un impact considérable sur les cantons et les communes. D'une part, les données concernées sont celles qui relèvent de la législation cantonale sur la protection des données. D'autre part, il s'agit de procédures pénales qui relèvent principalement de la compétence des cantons. Même si la Confédération peut, sur la base de sa compétence en matière d'affaires étrangères (art. 54, al. 1 Cst.), conclure également des traités internationaux dans des domaines qui relèvent de la compétence des cantons, elle doit impérativement associer ces derniers si elle veut prendre des décisions de politique extérieure « affectant leurs compétences ou leurs intérêts essentiels » (art. 55, al. 1 Cst.). Dans ce cas, le Conseil fédéral doit informer les cantons en temps utile et de manière détaillée et il doit les consulter (art. 55, al. 2 Cst.). Ce serait vraisemblablement le cas pour la conclusion d'un *executive agreement.*

5.3 Notion de « *serious crime* » (infraction grave)

Les *executive agreements* peuvent servir de base à l'acquisition d'informations aux fins de prévention, de détection, d'enquête et de poursuite de *serious crimes*[59]. Les infractions qui constituent des *serious crimes* au sens de l'*executive agreement* peuvent être par exemple clarifiées par le biais d'une liste d'infractions ou par la mention d'une peine minimale dans l'*executive agreement*.

La première variante (liste d'infractions) présente l'inconvénient d'être statique. La liste doit être constamment mise à jour et des contradictions pourraient apparaître en cas de modification de la loi.

La seconde variante (mention d'une peine minimale) est dynamique, mais contient un champ d'application potentiellement plus large (p. ex. tous les crimes et délits). Le fait que les infractions ne soient pas nécessairement qualifiées de la même manière dans les différents États se révèle être un défi. Si un acte est passible d'une peine élevée dans un État, il peut être puni de manière plus clémente ou ne pas l'être du tout dans un autre État. La question se pose donc de savoir si le critère des *serious crimes* doit être rempli dans les deux États, et donc si l'on applique une double incrimination « qualifiée » en conséquence, ou si l'accès aux

[57] RS **101**

[58] RS **172.010**

[59] DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 5.

données auprès d'un CSP est toléré même si l'acte n'est pas répréhensible dans son propre État.

Compte tenu de l'engagement toujours très fort des USA dans la lutte contre le terrorisme, il est prévisible qu'une couverture complète de la coopération dans le cas du « terrorisme » serait en tout cas un objectif américain pour un éventuel *executive agreement.* Cela n'est pas sans poser problème dans le contexte de la définition éventuellement plus étroite de l'organisation terroriste dans l'art. 260ter CP[60] révisé. Des évaluations différentes particulièrement marquées et politiquement sensibles existeraient probablement dans le domaine de la *délinquance fiscale*. L'irrecevabilité générale de la *fraude fiscale* (cf. art. 3, al. 3 EIMP) n'est guère compatible avec les intérêts des USA. Il pourrait en être de même pour le domaine des *infractions contre l'honneur*. Aux USA, il existe une très grande liberté d'expression (*freedom of speech*), qui inclut en principe les discours de haine (*hate speech*), pour autant qu'ils ne soient pas considérés comme un appel direct à la violence. De nombreux discours de ce type auraient depuis longtemps été sanctionnés en Suisse, notamment au titre du délit de discrimination raciale (art. 261bis CP).

Il semble donc qu'il serait difficile de trouver un standard commun pour le concept de « *serious crimes »* entre la Suisse et les USA.

5.4 Collecte de données électroniques

L'objectif du *CLOUD Act* et d'un *executive agreement* est de permettre la collecte transfrontière de données électroniques. Une question importante est donc de savoir quelles données peuvent être collectées auprès de qui et comment. De cette manière, il est possible d'évaluer si les modalités de collecte sont compatibles ou si elles doivent être adaptées.

Aux USA comme en Suisse, la législation vise les fournisseurs de services de télécommunication et les fournisseurs de services connexes.

5.4.1 Destinataires

La législation américaine établit une distinction entre les fournisseurs de services de communication électronique (*electronic communication services*) et ceux de services informatiques à distance (*remote computing services*). Un service de communication électronique correspond à toute offre de service qui permet à l'utilisateur d'envoyer ou de recevoir des communications filaires ou électroniques (*wire or electronic communications*)[61]. Les communications filaires sont des communications faisant appel à la voix humaine[62]. Les communications élec-

60 Cf. FF **2020** 7891.

61 « [A]ny service which provides to users thereof the ability to send or receive wire or electronic communications » (18 USC § 2510(15)).

62 « ‹[W]ire communication› means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce » (18 USC § 2510(1)). « ‹[A]ural transfer› » means a transfer containing the human voice at any point between and including the point of origin and the point of reception » (18 USC § 2510(18)).

troniques s'effectuent via le transfert de données et à l'exclusion de toute communication faisant appel à la voix humaine[63]. Les services informatiques à distance comprennent la fourniture publique de capacité de stockage ou de puissance de processeur par un service de communication électronique[64].

La Suisse fait une distinction entre les fournisseurs de services de télécommunication (« FST ») et les services de communication dérivés. Les services de télécommunication impliquent la « transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication »[65], tandis que les services de communication dérivés « sont supportés par des services de télécommunication et permettent une communication unilatérale ou multilatérale »[66]. Selon le message du Conseil fédéral, on entend par communication unilatérale le téléchargement ou le traitement en ligne de documents (p. ex. Google Docs ou Microsoft Office en ligne). Ainsi, les services de communication dérivés comprennent des offres d'hébergement web, des plateformes d'échange de documents et, enfin et surtout, des services de cloud[67]. La communication multilatérale fait référence aux interactions entre les utilisateurs, au moyen de courriers électroniques, d'une messagerie instantanée ou d'une application VoIP comme Skype[68].

Dans ce contexte, la situation initiale dans les deux ordres juridiques (USA et Suisse) n'est certes pas « identique », mais elle n'est pas non plus différente au point qu'un accord sur une définition commune des destinataires dans un *executive agreement* serait impossible.

5.4.2 Type de données

Il existe également des points communs pour le type de données. De manière générale, on fait une distinction de part et d'autre de l'Atlantique entre les données personnelles, les données secondaires et les données de contenu. Les données personnelles (*basic subscriber information*[69]), telles que définies dans la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[70], fournissent des informations sur le client et la relation contractuelle avec le fournisseur[71]. Les données secondaires au sens de la LSCPT ou les métadonnées (*transactional data*) indiquent avec qui, quand et comment la personne est

63 « ‹[E]lectronic communication› means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include — (A) any wire or oral communication ; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title) ; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds » (18 USC § 2510(12)).

64 « [T]he term ‹remote computing service› means the provision to the public of computer storage or processing services by means of an electronic communications system » (18 USC § 2711(2)).

65 Art. 3, let. b Loi sur les télécommunications (LTC, RS **784.10**).

66 Art. 2, let. c Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS **780.1**).

67 Explicitement dans le message, FF **2013** 2708.

69 Celles-ci comprennent notamment le nom, l'adresse, le type et la durée du service utilisé, les instruments de paiement, y compris les numéros de carte de crédit et de compte : 18 USC § 2703(c)(2).

70 RS **780.1.**

71 Cf. la définition de l'art. 18 al. 3 de la Convention de Budapest : « [t]oute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de services ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. »

en communication[72]. Enfin, le contenu (*content*) fait référence au message oral ou écrit proprement dit. Plus l'intervention de l'État se rapproche du cœur de la communication, c'est-à-dire du contenu, plus elle est intrusive et, par conséquent, plus elle doit être justifiée. Aux USA et en Suisse, les données personnelles peuvent être collectées sans autorisation judiciaire. La collecte de données secondaires et de contenu nécessite une autorisation judiciaire dans les deux pays. En Suisse, la collecte de données secondaires ou de contenu est une mesure de contrainte, mais la collecte de données personnelles ne l'est pas.

5.4.3 Modalités de collecte

Même si jusqu'à présent, la situation a paru similaire dans les deux pays, il existe cependant une différence importante au niveau des modalités de collecte des données. En Suisse, la collecte est effectuée par le service chargé de la surveillance de la correspondance par poste et télécommunication (service SCPT)[73]. Celui-ci assure la fonction de plateforme entre les autorités et les CSPs : les ordres de surveillance et les données qui en découlent sont échangés via cette plateforme, si nécessaire avec l'autorisation du Tribunal des mesures de contrainte.

En revanche, le *CLOUD Act* part du principe que les CSPs sont directement sollicités et tenus de remettre les données. Cependant, cet accès direct aux CSPs poserait les problèmes suivants :

- Il serait contraire au système de permettre aux autorités américaines d'accéder directement aux CSPs alors que les autorités suisses doivent passer par le service SCPT. La question de l'égalité de traitement se pose. À cet égard, la question des coûts constitue un aspect important : les autorités suisses paient des frais élevés pour l'utilisation du service SCPT, qui ne seraient pas – ou pas de la même manière – encourus dans le cas d'un accès direct.
- Cela conduirait également à une collecte selon deux circuits : les CSPs, qui ont mis en place des procédures et des protocoles dans le cadre du SCPT pour les requêtes par le service SCPT, devraient servir parallèlement les autorités américaines par d'autres moyens.
- On peut se demander si la surveillance en temps réel serait possible de cette manière : la surveillance est généralement effectuée par le CSP sur ordre de l'autorité de poursuite pénale et sur décision du service SCPT, mais il suffit parfois qu'elle soit activée et tolérée par le fournisseur. Il semblerait que la surveillance nécessite des préparations techniques importantes, qui varient fortement d'un cas à l'autre. Par conséquent, on peut difficilement imaginer qu'elle puisse être réalisée dans le cadre d'une relation bilatérale entre une autorité américaine et un CSP suisse.
- Les décisions du service SCPT sont des décisions au sens de l'art. 5 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[74]. Le CSP concerné peut faire appel contre ces décisions (notamment contre celles ordonnant une surveillance pour exécuter un ordre de surveillance délivré/transmis par une autorité de poursuite

[72] Voir la définition à l'art. 8, let. b LSCPT: « les données indiquant avec qui, quand, combien de temps et d'où la personne surveillée a été ou est en communication ainsi que les caractéristiques techniques de la communication considérée ».

[73] « Service chargé de la surveillance de la correspondance par poste et télécommunication, conformément à l'art. 269 du code de procédure pénale suisse (CPP) », cf. art. 3 LSCPT.

[75] 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 ; JO L 119/2016 du 4 mai 2016.

pénale) dans un cadre restreint. Cette possibilité pourrait *de facto* être encore plus limitée, voire suspendue, si le service SCPT ne joue plus aucun rôle ou ne transmet plus ces décisions.

Il serait concevable d'accorder également aux autorités américaines un accès via le service SCPT. Cependant, cela signifierait une extension massive des tâches pour le service SCPT. En outre, le texte du *CLOUD Act* n'est pas « adapté » à cette solution car il suppose que les données sont collectées directement auprès du CSP (toutefois, les ajustements nécessaires pourraient éventuellement être convenus dans l'*executive agreement*).

Les avantages d'une solution via le Service SCPT seraient évidents : en ce qui concerne la collecte des données, une égalité de traitement entre les autorités américaines et suisses serait établie (p. ex. les mêmes frais devraient être facturés aux autorités américaines). En outre, les autorités américaines auraient un point de contact unique (*single point of contact*), ce qui est dans tous les cas un avantage dans le trafic international des données. En poussant encore plus loin le raisonnement, le service SCPT pourrait ainsi jouer le rôle d'une autorité centrale pour la collecte des données américaines. Il serait alors possible de répondre aux craintes concernant la perte de la fonction de surveillance de l'OFJ : dans le cas de l'accès direct, tel que prévu par le *CLOUD Act*, il n'est pas précisé qui vérifie les motifs d'exclusion applicables à l'entraide judiciaire, qui contrôle le respect du principe de spécialité, etc. Toutefois, la manière dont la protection juridique du côté suisse pourrait fonctionner, comme décrit plus loin, reste également à définir (cf. point 5.6).

5.5 Protection des droits fondamentaux, en particulier protection des données et de la vie privée

5.5.1 Niveau européen : lien entre le *CLOUD Act* et le règlement général de l'UE sur la protection des données (RGPD)

5.5.1.1 Compatibilité du *CLOUD Act* et du RGPD

La compatibilité entre le *CLOUD Act* et un éventuel *executive agreement* conclu sur les principes de ce texte, d'une part, et de l'autre le droit européen, en l'occurrence le règlement général sur la protection des données[75] (RGPD), en vigueur depuis 2018, présente aussi une grande importance pour la Suisse. La Suisse n'étant pas membre de l'UE, le RGPD ne s'y applique pas directement puisqu'il ne s'agit pas d'un développement de l'acquis de Schengen. Mais ses dispositions s'appliquent aux entreprises en Suisse qui selon l'art. 3 RGPD relèvent du champ d'application du règlement. C'est le cas lorsque le CSP fournissant ses services est établi dans l'UE, ou s'il n'y est pas établi, lorsque les traitements de données sont liés à l'offre de biens ou de services à des personnes concernées dans l'Union ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

Afin de pouvoir échanger des données personnelles avec l'UE et ses pays membres, la Suisse doit continuer à être reconnue par la Commission européenne comme pays tiers assurant un niveau de protection adéquat, conformément à l'art. 45 RGPD. Pour que la *décision d'adéquation* soit maintenue, il est impératif que le droit suisse soit adéquat aux exigences du règlement en matière de protection des données. L'évaluation de la compatibilité du *CLOUD Act* et de l'éventuel *executive agreement* conclu sur la base de cette loi avec le RGPD a donc des conséquences sur la décision d'adéquation de l'UE dont la Suisse a besoin. Ceci est cor-

[75] 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 ; JO L 119/2016 du 4 mai 2016.

roboré par le fait que la Commission européenne, dans son évaluation du caractère adéquat de la protection des données assurée par le Royaume-Uni selon le RGPD, a examiné l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act*, et plus particulièrement sa compatibilité avec la législation européenne relative à la protection des données[76]. En revanche, dans le présent contexte, la situation au regard de la directive (UE) 2016/680[77] relative à la protection des données dans le cadre pénal n'est pas analysée. Certes, cette directive relève de Schengen, et à ce titre, elle doit être appliquée par la Suisse. Cependant, elle n'entre pas en considération dans la mesure où le *CLOUD Act* règle la transmission de données de CSPs privés *aux* autorités de poursuite pénale et non la transmission de données *par* les autorités (de poursuite pénale), qui sont les destinataires (exclusifs) de la directive. Enfin, l'accord RU-USA *CLOUD Act* ne semble pas avoir eu de pertinence pour l'évaluation par la Commission européenne de l'adéquation du niveau de protection des données du Royaume-Uni au regard de la directive (UE) 2016/680[78].

En résumé, il ressort de l'examen des bases juridiques déterminantes que les traitements de données réalisés sur injonction d'une autorité de poursuite pénale américaine dans le cadre du *CLOUD Act* peuvent être qualifiés de problématiques du point de vue de leur *légalité*. Ceci est vrai tout autant de la conservation de données personnelles que de leur divulgation.

Certes, tout comme le Comité Européen de la Protection des Données (EDPB) et le Contrôleur européen de la protection des données (CEPD), la Commission européenne reconnaît elle aussi que sur la base de l'art. 6 et plus particulièrement de l'art. 49 RGPD, dans des situations exceptionnelles déterminées, un traitement de données, voire la transmission de données à un État tiers, peut être justifié même quand cet État ne dispose pas d'une décision d'adéquation de la Commission européenne ni de garanties appropriées relatives à la protection des données (art. 46 RGPD). Ce serait notamment le cas si la divulgation des données personnelles par le CSP était nécessaire à la *sauvegarde des intérêts vitaux de la personne concernée* (art. 6, al. 1, let. d en rapport avec art. 49, al. 1, let. f RGPD). Par ailleurs, il n'est pas exclu qu'un tel transfert de données puisse être justifié par des motifs importants d'intérêt public (art. 49, al. 1, let. d RGPD) reconnus dans l'UE et ses pays membres, par exemple dans l'hypothèse où il existerait des indications concrètes concernant une infraction pénale grave ou un attentat terroriste en préparation dans l'UE. Cependant, dans la pratique, on peut supposer que cette situation dérogatoire ne serait que très rarement constituée, le RGPD ne permettant de tels transferts liés à des risques particuliers pour les droits et les libertés des personnes concernées qu'à des conditions très strictes et dans des situations absolument exceptionnelles.

---

[76] Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni ; C(2021) 4800 final, chiffres 153-156.

[77] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ; JO L119/89 du 4.5.2016.

[78] Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément à la directive (UE) 2016/680 du Parlament européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni : C(2021) 4801 final. Afin de prendre en compte l'avis 15/2021 du Comité Européen de la Protection des Données sur la décision d'adéquation du Royaume-Uni selon la directive (UE) 2016/680, qui porte un regard extrêmement critique sur les injonctions de surveillance par écoute, notamment celles figurant dans l'accord bilatéral conclu par le Royaume-Uni et les USA sur le *CLOUD Act*, la Commission européenne a complété sa décision. Dans le cadre de la surveillance des futures évolutions concernant la protection des données au Royaume-Uni, elle accordera une attention particulière à la conclusion d'accords internationaux ayant des effets sur le niveau actuel de protection des données (point 165 de cette décision). Cependant, même si la directive (UE) 2016/680 est interprétée dans l'UE comme portant non seulement sur les transmissions de données, mais aussi sur les traitements de données effectués par des autorités de poursuite pénale, le champ d'application de cette directive est interprété de manière plus étroite en Suisse, et ne nous semble pas remis en cause présentement.

De même, le traitement des données sur la base du *CLOUD Act* pourrait s'avérer problématique en ce qui concerne d'autres éléments clés du RGPD :

Du point de vue de la transparence, le fait que les autorités américaines de poursuite pénale ne soient pas obligées, dans certains cas, d'informer les personnes concernées de la communication des données, et qu'elles puissent même, par voie de décision judiciaire, obliger le CSP à ne pas en informer la personne concernée, pourrait être problématique[79]. Dans la conception européenne du droit, même en matière de poursuite pénale et d'exécution des peines, on considère qu'il est impératif que la personne concernée soit informée de l'accès des autorités à ses données personnelles[80]. Selon la Cour de justice de l'UE (CJUE), la personne concernée doit être informée de la communication de ses données personnelles à des autorités étrangères de poursuite pénale, au plus tard lorsque cela ne risque plus de nuire aux investigations correspondantes[81].

Du point de vue de la proportionnalité, le EDPB et le CEPD parviennent à la conclusion que dans l'ensemble, le *CLOUD Act* respecte ce principe[82]. Ainsi, une autorité américaine de poursuite pénale ne peut exiger la divulgation de données personnelles que si un tribunal l'a au préalable autorisée et si l'autorité expose, dans une déclaration sur l'honneur, qu'elle dispose de suffisamment d'éléments pour soupçonner qu'un crime défini a été commis ou est en train d'être commis et que les informations réclamées contiennent la preuve de ce crime précis[83]. L'injonction de production doit en outre contenir une description exacte des données personnelles demandées, les recherches à l'aveuglette ou *fishing expeditions* destinées à trouver des preuves n'étant pas admises[84]. Mais les autorités européennes de protection des données constatent aussi que dans le cas d'autres formes de requêtes, aucun contrôle judiciaire correspondant n'est exigé[85]. Il faudrait ici décider au cas par cas si un traitement de données est proportionnel ou pas.

Contrairement au RGPD, qui accorde la même protection aux données personnelles de toutes les personnes physiques, quelle que soit leur nationalité ou leur lieu de résidence, le *CLOUD Act* fait une distinction entre les données des *US persons* et celles des autres personnes. En particulier dans le cas où il existe un *executive agreement*, un CSP ne peut exiger le contrôle judiciaire d'une injonction émanant d'une autorité américaine de poursuite pénale en cas d'obligations juridiques contradictoires, que s'il ne s'agit pas de données personnelles de *US persons* [86]. En revanche, selon le CEPD, toute inégalité de traitement fondée sur la nationalité ou le lieu de résidence de la personne concernée est incompatible avec le RGPD[87].

Le *CLOUD Act* ne prévoit pas de garanties en matière de protection des données pour les personnes concernées, par exemple sous la forme d'un droit d'accès ou d'un droit de consultation de leurs données. Au contraire, il permet de renoncer entièrement, dans certains cas, à informer les personnes concernées que des données les concernant ont été transmises à

---

79 *CLOUD Act,* § 2703 (b) (1) et § 2705 (b).

80 Cf. entre autres CJUE, Avis 1/15 Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220 et avis 23/2018 du CEPD, p. 19.

81 CJUE, Avis 1/15 Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220.

82 EDPB/CEPD, Initial legal assessment, p. 2.

83 DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act* », p. 8.

84 Idem, p. 8.

85 EDPB/CEPD, Initial legal assessment, p. 2.

86 *CLOUD Act,* § 2703.

87 Avis 2/2019 du CEPD, chiffre 50.

une autorité américaine de poursuite pénale[88]. Cela va à l'encontre de l'art. 8, al. 2 de la Charte européenne des droits fondamentaux[89], qui garantit explicitement le droit pour toute personne d'accéder aux données personnelles collectées la concernant et d'en obtenir la rectification.

Le *CLOUD Act* ne prévoit aucune possibilité, pour la personne concernée par une injonction de production, de se défendre face à la divulgation de ses données personnelles. Dans les cas de conflits de droit, une possibilité restreinte de défense est uniquement prévue pour le CSP, et seulement à la condition qu'un *executive agreement* ait été conclu entre les USA et l'État correspondant[90]. En revanche, la personne concernée par une injonction de ce type ne peut ni saisir une autorité de contrôle indépendante, ni exercer un recours judiciaire pour s'opposer à la transmission. L'absence de droit à un recours effectif devant un tribunal est contraire à l'art. 47 de la Charte européenne des droits fondamentaux, qui garantit le droit à une protection juridique et judiciaire efficiente. La CJUE insiste par ailleurs sur l'importance, pour toute personne concernée, de pouvoir déposer un recours administratif auprès d'une autorité nationale de contrôle[91].

L'art. 8, al. 3 de la Charte européenne des droits fondamentaux prévoit, comme garantie essentielle de la protection des données, un contrôle exercé par une autorité indépendante. À cet égard, le CEPD insiste sur le fait que les autorités compétentes de l'État sur le territoire duquel se trouvent les données personnelles demandées doivent être impliquées dans les processus de transmission de preuves électroniques, afin de garantir efficacement la protection des droits fondamentaux[92]. De la même manière, les autorités compétentes en matière de protection des données devraient elles aussi être informées, en cas d'injonctions directement adressées aux prestataires, de manière à pouvoir exercer un contrôle[93]. Dans ce contexte, le fait que les CSPs transmettent des données personnelles à une autorité américaine de poursuite pénale sans en informer les autorités compétentes de leur propre pays pourrait se révéler problématique.

5.5.1.2 Bilan : risques liés à la conclusion d'un *executive agreement* avec les USA pour la décision d'adéquation de la Suisse

La *décision d'adéquation* évoquée au chiffre 5.5.1.1 est évaluée régulièrement par la Commission, à savoir au moins tous les quatre ans (art. 97 RGPD). Les principaux aspects pris en compte lors de cet examen sont les règles de protection des données, les règles concernant la transmission de données personnelles vers un pays tiers et la conclusion d'accords internationaux relatifs à la protection des données personnelles. Dans l'arrêt *Schrems II*, la CJUE a précisé, en ce qui concerne l'accès des autorités aux données personnelles transmises dans l'État destinataire à des fins de sécurité nationale, que la Commission, pour prendre sa décision, doit tenir compte du droit national applicable dans l'État destinataire. Le critère décisif de l'adéquation est de savoir si la réglementation qui autorise l'ingérence des autorités dans l'État destinataire à des fins de sécurité nationale contient également des dispositions claires sur la limitation de cette ingérence, et donc précise clairement à quelles conditions et dans quelles circonstances elle peut être permise. L'accès aux données doit s'opérer

88 *CLOUD Act* § 2703 (b) (1) et § 2705 (b).

89 Charte européenne des droits fondamentaux, JO 2000/C 364/01 du 18.12.2000.

90 Cf. plus haut, chiffre 3.2.2.

91 Arrêt de la CJUE, *Maximillian Schrems contre Data Protection Commissioner*, C-362-14, ch. marg. 56 – 58.

92 Avis 2/2019 du CEPD, chiffre 28. Dans le contexte des injonctions européennes de production et de conservation de preuves électroniques en matière pénale, voir aussi l'avis 23/2018 du EDPB, p. 16.

93 Voir l'avis 23/2018 du EDPB, p. 8.

dans les limites du strict nécessaire[94]. D'autre part, la réglementation correspondante doit prévoir dans l'État destinataire des droits effectifs et opposables afin de protéger les personnes concernées contre d'éventuels abus[95].

En 2000, la Suisse a reçu de l'UE la confirmation qu'elle offrait un niveau de protection des données adéquat. Pour l'instant, cette décision d'adéquation continue d'être valable sous l'angle du RGPD, applicable depuis le 25 mai 2018. Au printemps 2019, la Commission européenne a commencé une nouvelle évaluation de la Suisse. Elle réalise cet examen sur la base du droit suisse en vigueur, mais s'est déclarée prête à prendre en compte le renforcement de la protection des données qu'entraînera la révision de la loi fédérale sur la protection des données (LPD), à condition que la révision totale de cette dernière soit achevée en temps utile. La nouvelle loi fédérale sur la protection des données (nLPD) ayant été adoptée par les Chambres fédérales le 25 septembre 2020 (voir plus bas, 5.5.2.1), et son entrée en vigueur, comme celle des ordonnances correspondantes, étant prévues pour le second semestre 2022, cette condition devrait être remplie.

Dans sa décision concernant le caractère adéquat du niveau de protection des données personnelles assuré par le Royaume-Uni conformément au RGPD, qui a été adoptée le 28 juin 2021 par la Commission européenne en même temps que la décision sur l'adéquation du Royaume-Uni selon la directive (UE) 2016/680, la Commission a évalué également l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act*[96]. Cela montre que le contenu d'un *executive agreement* conclu entre la Suisse et les USA serait lui aussi pris en compte dans la perspective d'une nouvelle évaluation du caractère adéquat du niveau de protection des données garanti par la Suisse.

Dans la décision relative au Royaume-Uni, la Commission européenne note que lors de l'entrée en vigueur de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act*, les données transférées depuis l'UE vers des CSPs au Royaume-Uni pourraient faire l'objet d'injonctions de production émanant des autorités de poursuite pénale des USA. Une évaluation des conditions et des garanties auxquelles de telles injonctions peuvent être exécutées est donc pertinente dans la perspective de la décision d'adéquation du niveau de protection des données garanti par le Royaume-Uni. Certes, la Commission n'estime pas que l'accord, au regard des exigences du RGPD, soit inadéquat en tant que tel. D'une part, la Commission européenne souligne qu'elle est elle-même mandatée par les pays membres pour mener des négociations avec les USA dans ce domaine, et que de ce fait, il ne faudrait pas créer de « *double standard* » quant à un accord correspondant entre le Royaume-Uni et les USA. D'autre part, la Commission juge positives les exigences strictes fixées dans l'accord en matière d'injonctions de production et de surveillance en temps réel, de même que le fait que par un renvoi à l'accord-cadre conclu entre l'UE et les USA[97], toutes les garanties et les droits définis dans ce dernier soient applicables par analogie[98]. La Commission retient en outre que les autorités britanniques lui ont confirmé que l'accord n'entrerait en vigueur que lorsque le respect de ces standards en matière de protection des données serait garanti pour toutes les données transférées dans le cadre de cet accord.

---

94 CJUE, *Schrems II,* consid. 175-176.

95 CJUE, *Schrems II,* consid. 177-178.

96)» (. Chiffres 153 - 156 de la décision sur l'adéquation relative au Royaume-Uni selon le RGPD.

97 Voir la note de bas de page 41

98 L'art. 9, al. 1 de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act* note qu'une protection équivalente à celle prévue par cet accord-cadre « s'applique à toutes les données personnelles collectées lors de l'exécution d'injonctions produites sur la base de l'accord. »

Le EDPB[99] et le Parlement européen[100] se montrent nettement plus sceptiques. Ils doutent, notamment, qu'une simple référence à l'accord-cadre UE-USA suffise pour que les droits en matière de protection des données qui y sont garantis puissent être effectifs et opposables selon le droit britannique et que les mesures de protection qui y sont prévues s'appliquent à toutes les injonctions de production des autorités américaines de poursuite pénale – et se demandent donc si le droit américain ne prévaudrait pas tout de même. Face à ces craintes, la Commission affirme que la décision d'adéquation prévoit une surveillance permanente des évolutions relatives à ces questions. Elle précise qu'elle accordera une attention particulière à l'application et à la mise en œuvre des garanties contenues dans l'accord-cadre lors des transferts de données correspondants, et tirera les conséquences qui s'imposent si certains signes indiquent qu'un niveau de protection adéquat n'est plus garanti. Une mesure essentielle préconisée à cet égard par la Commission européenne est la *« sunset clause* », qui figure à l'art. 4 de la décision d'adéquation, et selon laquelle la décision d'adéquation du niveau de protection garanti par le Royaume-Uni expirera automatiquement au bout de quatre ans, si aucun accord supplémentaire n'est adopté.

Même si, selon la Commission européenne, l'accord entre le Royaume-Uni et les USA garantit les standards de protection des données applicable dans l'UE, , la situation de départ est différente pour la Suisse. De fait, le Royaume-Uni, à l'exception du domaine du contrôle de l'immigration[101], applique encore l'intégralité du RGPD, du moins pour l'instant – ce qui n'est pas le cas de la Suisse. De plus, la référence à l'accord-cadre conclu entre l'UE et les USA et l'affirmation correspondante des autorités britanniques de ne laisser entrer en vigueur l'accord que si les garanties correspondantes sont assurées, permettent à la Commission de considérer que les données personnelles transmises sur la base de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act* continuent à bénéficier de la protection d'un instrument juridique de l'UE.

À cet égard, les possibilités pour la Suisse semblent plus limitées. Du fait du cadre étroit et problématique du point de vue de la protection des données du *CLOUD Act*, on ne peut supposer que la Suisse, par la conclusion d'un *executive agreement*, pourrait satisfaire aux exigences décrites plus haut dans le domaine de la protection des données. C'est pourquoi, la Commission, en menant ses propres négociations avec les USA, poursuit l'objectif d'un accord global qui règlerait les échanges de preuves électroniques et irait donc plus loin qu'un *executive agreement* tel que le *CLOUD Act* le prévoit. La Suisse ne pourrait donc sans doute obtenir la protection juridique complète, qui est exigée par la législation européenne en matière de protection des données et qui est garantie dans le cas du Royaume-Uni selon l'avis de la Commission, que par la conclusion d'un accord *global* avec les USA. Cet accord devrait réglementer les échanges de preuves électroniques et prévoir simultanément un haut niveau de protection des données correspondant aux standards européens et nationaux. Enfin, pour satisfaire également aux exigences de l'EDPB, il faudrait garantir qu'un tel accord *prévale sur le droit américain* en cas d'échange de données entre un CSP et des autorités de poursuite pénale.

---

[99] Avis 14/2021 du 13 avril 2021 du EDPB sur le projet de décision d'exécution de la Commission européenne constatant, conformément au règlement (UE) 2016/679, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, ch. marg. 88 ss

[100] Résolution du Parlement européen du 21 mai 2021 sur le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (2021/2594 (RSP)), ch. 25.

[101] Compte tenu de l'arrêt de la *Court of Appeal* du Royaume-Uni du 26 mai 2021, par lequel les réglementations d'exception des prétentions relatives à la protection des données prévues au Royaume-Uni dans le domaine du contrôle de l'immigration sont jugées incompatibles avec le RGPD, la Commission européenne exclut dans un premier temps ce domaine de la décision d'adéquation prévue conformément au RGPD. Dès qu'il sera établi que le Royaume-Uni corrigera ces défauts, et de quelle manière, la Commission étudiera la possibilité d'une réintégration de ce domaine et modifiera éventuellement la décision en conséquence (chiffre 6 de la décision sur l'adéquation relative au Royaume-Uni selon le RGPD).

En outre, on peut supposer que la Commission européenne accordera, pour les futures décisions d'adéquation, plus de poids aux réserves formulées par l'EDPB et le Parlement européen au sujet de l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act* que dans le cas du Royaume-Uni. Ici, l'urgence de trouver une base juridique aux transferts de données depuis l'UE vers le Royaume-Uni à l'issue de la période de transition semble avoir été un facteur déterminant qui a poussé la Commission à ne pas dévier de son projet, malgré la résistance du Parlement et de l'EDPB, d'adopter les décisions d'adéquation relatives au Royaume-Uni avant la fin du mois de juin 2021. Comme déjà mentionné, ces décisions ont été adoptées le 28 juin 2021 et sont de durée limitée, valides jusqu'en 2025.

Dans ses décisions d'adéquation relatives au Royaume-Uni, la Commission européenne insiste sur le fait qu'elle appuie pour l'essentiel ses évaluations sur l'arrêt *Schrems II* de la CJUE (arrêt du 16 juillet 2020). Cela devrait inciter la Suisse à adopter une démarche prudente, étant donné que la Cour de justice y indique que la Commission européenne, dans sa décision sur le caractère adéquat de la communication de données aux USA dans le cadre du *Privacy-Shield*, n'a pas tenu compte du fait que les dispositions relatives aux programmes de surveillance nationaux n'offrent, selon le droit américain, pas de garanties suffisantes de respect des exigences du RGPD en matière de protection des données, et pas non plus de protection juridique suffisante aux personnes concernées n'entrant pas dans la catégorie des *US persons*[102]. On peut en déduire que la Commission européenne sera encore plus stricte, lors de ses futures décisions d'adéquation, dans l'évaluation des garanties offertes par les accords internationaux pour combler de telles lacunes en matière de protection des données. En outre, les alignements d'autres actes juridiques sur la directive (UE) 2016/680[103], entrepris actuellement dans le domaine des poursuites pénales et de l'exécution des peines, montrent qu'à l'avenir, l'UE sera encore plus stricte dans son application des conditions d'échanges de données dans ces domaines.

5.5.2 Licéité du traitement des données et des divulgations fondées sur une injonction de production basée sur le *CLOUD Act* sous l'angle du droit suisse

5.5.2.1 Aspects pertinents du cadre juridique de la protection des données en Suisse

Au niveau fédéral, la protection des données est actuellement régie prioritairement par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[104]. L'objet de la LPD est le traitement des données par les organes fédéraux comme par les personnes physiques. En outre, de nombreux standards de protection des données spécifiques à des domaines particuliers contenus dans des lois spéciales règlent les traitements de données effectués par les organes de la Confédération. Pour le traitement de données par les organes fédéraux et les particuliers, d'autres textes s'appliquent également, à savoir l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)[105] et l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD[106]). Le traitement de données par des organes cantonaux ou communaux est réglé dans les lois cantonales relatives à la protection des données.

[102] CJUE, *Schrems II,* consid. 175-178.

[103] Cf. « Communication from the Commission to the European Parliament and the Council ; Way forward on aligning the former third pillar acquis with data protection rules », disponible sur https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v7.pdf (version 7.6.2021).

[105] RS **235.11**

[105] RS **235.11**

[106] RS **235.13**

Le 25 septembre 2000, le Parlement a adopté la révision totale de la LPD (nLPD)[107]. La consultation sur l'OLPD révisée est en cours. En l'état actuel des choses, l'entrée en vigueur de la législation révisée relative à la protection des données est prévue pour le second semestre 2022. Avec cette révision totale, la législation suisse sur la protection des données sera considérablement renforcée et rapprochée du niveau de protection européen.

Dans la question de la compatibilité du traitement des données effectué sur la base d'injonctions de production avec la législation suisse en matière de protection des données, les textes déterminants sont la LPD en vigueur, l'OLPD ainsi que les dispositions pertinentes de la LPD totalement révisée (OLPD incluse). En revanche, dans le présent contexte, il n'est pas nécessaire de prendre spécialement en compte la loi fédérale du 28 septembre 2018 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS)[108], compte tenu de son champ d'application, ni la Convention révisée 108+ du Conseil de l'Europe, ratifiée par la Suisse. Par son contenu, cette dernière est très proche de la directive (UE) 2016/680 et du RGPD ; les principes qui y sont énoncés ont été pris en compte dans le cadre de la révision de la LPD.

5.5.2.2 Aspects problématiques au regard des principes de la protection des données en Suisse

La législation suisse sur la protection des données repose sur un autre présupposé que le RGPD, selon lequel le traitement de données par des personnes physiques est fondamentalement illicite à moins qu'il ne soit dûment justifié par un motif valable. En Suisse, les traitements de données effectués par des personnes privées sont autorisés pour autant qu'ils ne portent pas atteinte à la personnalité. Il y a notamment atteinte à la personnalité quand un traitement de données enfreint les principes généraux de l'art. 4 LPD/art. 6 nLPD (en particulier la licéité, la bonne foi, la proportionnalité, le traitement limité au but indiqué et les finalités reconnaissables pour la personne concernée) ou que les exigences en matière d'exactitude des données (art. 5 LPD/art. 6, al. 5 nLPD) et de sécurité des données (art. 7 LPD/art. 8 nLPD) ne sont pas remplies (art. 12, al. 2, let. a LPD, art. 30, al. 2, let. a nLPD)[109]. En général, ces principes sont repris tels quels dans la législation révisée. En sus de ces principes de protection des données, les divulgations de données à l'étranger doivent respecter les exigences de l'art. 6 LPD[110], qui ont été reprises aussi dans le droit révisé (art. 16 s. nLPD).

Au regard des principes de protection des données, les traitements de données effectués sur la base du *CLOUD Act* semblent problématiques à différents égards. Ainsi, le principe de la bonne foi exige que les règles générales liées au traitement des données s'appliquent. Ceci reste valable lorsque les prescriptions et garanties se rapportant à la protection des données sont incomplètes ou ne sont pas concrètes. Ceci concerne notamment la question de la transparence du traitement des données. Dans ce contexte, les traitements de données effectués suite à des injonctions de production pourraient être problématiques à plusieurs égards. La divulgation de données en dehors du cadre d'une requête d'entraide judiciaire peut être considérée comme une infraction au principe de la bonne foi. Et on peut en dire autant des traitements de données qui se font à l'insu de la personne concernée[111]. Une autre

[107] FF **2020** 7397

[108] RS **235.3**

[109] BRUNO BAERISWYL dans : BAERISWYL BRUNO (Éditeur), Stämpflis Handkommentar zum Datenschutzgesetz (SHK DSG), Berne 2015, remarques préliminaires concernant l'art. 4 – 11*a*, ch. marg. 3.

[110] MAURER-LAMBROU/STEINER dans BSK DSG et BGÖ, art. 6 LPD, ch. marg. 11a.

[111] Message LPD, FF **1988** II 421 (457).

disposition du *CLOUD Act* pourrait se révéler problématique, à savoir celle qui interdit totalement d'informer la personne concernée avant que les autorités n'accèdent aux données.

Il découle du principe de proportionnalité que seules les données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Il doit y avoir un rapport raisonnable entre les finalités et le moyen utilisé, et les droits de la personne concernée doivent être préservés dans la plus large mesure possible[112]. Ce principe s'applique aussi aux personnes physiques qui traitent des données. Il convient en cela de toujours concilier les intérêts des personnes concernées et ceux du responsable du traitement. Dans la mesure où le *CLOUD Act* prévoit une vérification judiciaire dans le cadre des injonctions de production (voir le point 3.2.1), on peut partir du principe que le principe de proportionnalité est bien respecté. En revanche, le fait que, pour d'autres formes de requêtes, aucun contrôle de ce type ne soit prévu pourrait se révéler problématique du point de vue de la proportionnalité. Par ailleurs, pour ce qui est de la nécessité, il convient d'examiner si la voie de la requête d'entraide judiciaire classique n'aboutirait pas au même résultat, et s'il ne faudrait pas la privilégier dans la mesure où elle constituerait une mesure plus « douce », entraînant une atteinte moins radicale aux droits de la personnalité de la personne concernée.

Les données doivent toujours être collectées pour des finalités déterminées et reconnaissables pour la personne concernée. Lorsque des personnes physiques traitent des données personnelles, la finalité de ce traitement est principalement déterminée par les informations fournies à la personne concernée lors de la collecte de ses données ou qui ressortent des circonstances. La personne concernée doit pouvoir comprendre ce qu'il advient de ses données. Un traitement ultérieur des données personnelles pour une finalité différente, que les personnes concernées peuvent légitimement considérer comme inattendu ou non reconnaissable, violerait leur droit à la vie privée et à l'autodétermination en matière d'information, à moins que ce changement de finalité ne soit justifié, par exemple, par leur consentement. Si des données personnelles sont conservées ou communiquées à des autorités américaines de poursuite pénale sur la base d'injonctions de production telles que celles prévues par le *CLOUD Act*, cela représente une modification de la finalité initialement prévue par les CSPs dans le cadre de leurs prestations contractuelles. Dans pareil cas, la loi exige que cette modification de finalité soit dument justifiée par un motif et que les personnes concernées en soient informées.

Le principe de reconnaissabilité exige que la collecte des données, comme les finalités du traitement, soient reconnaissables pour la personne concernée. Ce principe est la condition du droit à l'autodétermination en matière d'information et de l'exercice des droits liés à la protection des données. Il découle de ce principe que les responsables du traitement sont tenus d'informer les personnes concernées, à moins que le traitement de leurs données ne soit pour elles clairement reconnaissable[113]. Sous cet angle aussi, les traitements de données effectués sur la base d'injonctions de production émanant des autorités des USA paraissent problématiques puisqu'elles s'appuient sur un droit étranger. De plus, il faudrait aussi examiner si le fait qu'une autorité américaine de poursuite pénale puisse interdire à un CSP, par voie de décision judiciaire, d'informer la personne concernée de la transmission de ses données pourrait être compatible avec le principe de transparence ou éventuellement justifié. L'information doit cependant être donnée au plus tard dès que cela ne risque plus de nuire à d'éventuelles investigations.

[112] Message LPD, FF **1988** II 421 (458).

[113] BAERISWYL, SHK DSG, art. 4, ch. marg. 47-50.

5.5.2.3 Motifs justificatifs pour les personnes physiques en cas d'atteinte à la personnalité, art. 13 LPD/art. 27 nLPD

Les motifs possibles justifiant qu'un traitement de données ne soit pas considéré comme une atteinte à la personnalité illicite sont : le consentement de la personne concernée, un intérêt prépondérant privé ou public, ou un traitement justifié par la loi. Cependant, selon la jurisprudence du Tribunal fédéral, une infraction aux principes de protection des données de l'art. 4, de l'art. 5, al. 1 et de l'art. 7, al. 1 LPD (ou art. 6 et 8 nLPD) ne peut être justifiée que dans de très rares cas[114].

Une atteinte à la personnalité peut être justifiée par le fait que la personne concernée consent au traitement des données. Pour que ce consentement soit juridiquement valable, il faut que la personne concernée ait été correctement informée de ce traitement de données. Ces informations doivent lui permettre d'évaluer les risques qui existent pour ses droits de la personnalité. Pour être correcte, l'information doit donc aussi mentionner les risques spécifiques d'une transmission à l'étranger et évoquer l'absence de dispositions appropriées en matière de protection des données. De plus, le consentement doit être librement donné, ce qui signifie que la personne concernée soit pouvoir se prononcer pour ou contre le traitement des données en dehors de toute pression[115]. Plusieurs auteurs affirment en outre qu'un consentement ne peut être libre que si la personne dispose d'une alternative non entachée d'inconvénients inacceptables[116].

Dans le présent contexte, il est problématique que lors de traitements des données effectués sur la base d'injonctions de production, il n'y ait pas de lien entre la prestation que le CSP doit fournir au client et le traitement des données requis à cet effet. Le client devrait donc consentir à cette finalité non indispensable à la fourniture de la prestation afin de pouvoir prétendre à celle-ci. Si un contrat est subordonné au consentement à un traitement des données non indispensable à l'exécution du contrat, le droit européen présuppose que ce consentement n'a pas été librement donné. Pour les traitements de données effectués dans le cadre des poursuites pénales et de l'exécution des peines, on peut en outre partir du principe que la personne concernée n'a pas de véritable liberté de choix. Cela indique pour le moins que l'exigence d'un consentement juridiquement valable en rapport avec le *CLOUD Act* ne devrait pas être remplie, et un CSP ne pourrait invoquer le consentement de la personne concernée comme motif justificatif pour des traitements et des transmissions de données effectués sur la base d'injonctions de production.

Les responsables du traitement privés peuvent eux aussi invoquer un intérêt prépondérant privé ou public pour justifier un traitement des données portant atteinte à la personnalité. L'élément déterminant est cependant que dans le cadre d'une pesée des intérêts, les intérêts concernés soient mis en balance et que dans le résultat, l'intérêt privé ou public ait plus de poids que l'intérêt de la personne concernée par l'atteinte à la personnalité. L'art. 13, al. 2 LPD ou l'art. 31, al. 2 nLPD fournissent une liste (non exhaustive) de possibles intérêts prépondérants du responsable du traitement.

Outre les éventuels intérêts de tiers ou, à titre exceptionnel, l'intérêt de la personne concernée elle-même, l'*intérêt direct* du responsable du traitement peut justifier un traitement des données[117]. Dans le contexte de traitements des données effectués sur la base d'injonctions

---

[114] BGE 136 II 508, consid. 5.2.4.

[115] BAERISWYL, SHK DSG, art. 4, ch. 65.

[116] Cf. RAMPINI dans BSK DSG, art. 13, ch. 6.

[117] WERMELINGER, A., « Art. 13 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpflis Handkommentar*, Berne : Stämpfli 2015, ch. 11.

de production, une justification dans l'intérêt propre du CSP devrait être examinée dans l'hypothèse où en cas de non-respect de l'injonction, il devrait s'attendre à des sanctions selon le droit américain. Ainsi, la Commission européenne, dans son « amicus brief » (requête) dans l'affaire Microsoft devant la Cour suprême des USA, a jugé possible, dans ce cas, un intérêt légitime du CSP. Mais même dans un contexte national, une conservation ou une transmission de données ne devrait être considérée comme licite que quand les intérêts de la personne concernée par l'atteinte à la personnalité ne sont pas prépondérants. Cependant, on ne peut s'attendre à ce qu'en cas de pesée des intérêts, un éventuel intérêt du CSP à ne pas être sanctionné serait prépondérant par rapport aux intérêts de la personne subissant l'atteinte à la personnalité. Cela revient à reconnaître que l'intérêt d'une personne à la protection de sa personnalité et de sa sphère privée et à l'autodétermination en matière d'information représente déjà *en soi* un intérêt de poids[118]. Dans la pesée des intérêts, il est probable que le fait que les USA offrent de moindres garanties en matière de protection des données ainsi que de moindres garanties procédurales pèse lui aussi lourdement dans la balance.

Comme exemples d'intérêts *publics* que des responsables du traitement privés peuvent faire valoir, on cite la sécurité ou la lutte contre le blanchiment d'argent[119]. Par intérêt public prépondérant, on entend ici l'intérêt public du point de vue de la Suisse. Ce dernier ne se limite pas exclusivement aux intérêts strictement nationaux ; au contraire, il peut aussi consister à soutenir les intérêts d'un pays étranger (par exemple dans la lutte contre le blanchiment d'argent), ou concerner les situations où les intérêts d'un pays étranger ont un « effet réflexe » sur la Suisse, et qu'il est donc, indirectement, dans l'intérêt de cette dernière de les soutenir[120]. Un intérêt étranger en matière de lutte contre le terrorisme, par exemple, pourrait ainsi représenter un intérêt public justifié du point de vue de la Suisse[121]. Sur ce point, la Suisse semble moins restrictive que l'UE avec le RGPD, selon lequel il ne peut y avoir d'intérêt public que si celui-ci est reconnu dans le droit de l'Union ou dans celui d'un État membre.

Si l'infraction grave (*serious crime*) poursuivie concrètement au moyen d'une injonction de production était reconnue comme relevant de l'intérêt public, et qu'une transmission de données était indispensable à cet effet, un CSP traitant des données personnelles à cet égard pourrait invoquer ce motif justificatif. Cet intérêt public doit toutefois être prépondérant par rapport à l'intérêt de la personne concernée subissant l'atteinte à la personnalité. Cependant, les traitements de données effectués sur la base d'injonctions émanant des autorités américaines de poursuite pénale devant fondamentalement être considérés comme incompatibles avec les principes de protection des données en vigueur ici, la protection des droits de la personnalité, de la sphère privée et de l'autodétermination en matière d'information de la personne concernée devrait peser fortement dans la balance lors de l'évaluation. Il faudrait donc placer la barre très haut dans l'évaluation de la proportionnalité de tels traitements de données.

Enfin, le traitement des données peut aussi être justifié par la loi, seule une base juridique relevant du droit suisse pouvant être prise en considération comme motif justificatif d'une éventuelle atteinte à la personnalité. Étant donné que dans le présent contexte, c'est un acte juridique américain, à savoir le *CLOUD Act*, qui sert de base juridique aux injonctions, un CSP ne pourrait pas invoquer la loi comme motif justificatif du traitement selon l'art. 13, al. 1 LPD ou l'art. 31, al. 1 nLPD. Cette situation ne pourrait probablement changer qu'avec la conclusion avec les USA d'un traité global sur les échanges de données incluant des standards

[118] ROSENTHAL, JÖHRI, art. 13, ch. 14 renvoie sur ce point à la jurisprudence du Tribunal fédéral, BGE **97** II 106 s.

[119] MAURER-LAMBROU, STEINER, « Art. 6 LPD », ch. marg. 32.

[120] ROSENTHAL, JÖHRI, art. 6, ch. marg. 60. Aussi BAERISWYL, B., BLONSKI, D., « Art. 6 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015, ch. marg. 30.

[121] Cf. p. ex. ROSENTHAL, JÖHRI, art. 6, ch. marg. 61.

de protection correspondants, qui satisferait aux exigences en matière de communication transfrontière des données (art. 6, al. 2, let. a LPD ou art. 16, al. 2, let. a nLPD). Un simple *executive agreement* selon le *CLOUD Act* ne suffirait guère à satisfaire ces exigences.

5.5.2.4 Compatibilité avec les exigences relatives à la communication transfrontière de données (art. 6 LPD/art. 16 et 17 nLPD)

Après avoir été communiquées à l'étranger, les données personnelles ne sont plus protégées par la législation suisse en matière de protection des données, mais soumises à un ordre juridique étranger, ce qui accroît le risque d'atteintes à la personnalité. L'art. 6 LPD impose des conditions à de telles communications de données susceptibles de menacer gravement la personnalité des personnes concernées. Il faut supposer ex lege que c'est le cas lorsque le pays concerné ne dispose pas d'une législation assurant une protection des données adéquate, c'est-à-dire d'une protection comparable à celle garantie par le droit suisse. Pour les USA, ce n'est pas le cas. Ainsi, le PFPDT considère que le niveau de protection offert par les USA n'est *plus adéquat dans aucun domaine*.

Dans la mesure où il a été constaté plus haut que les traitements de données effectués sur la base d'injonctions de production étaient globalement problématiques au regard des principes de protection des données, et qu'il était probable qu'ils soient illicites au regard de la législation suisse en matière de protection des données, il est superflu d'examiner leur compatibilité avec les exigences relatives à la communication transfrontière de données.

Mais pour résumer, on peut retenir ceci : même en l'absence de protection adéquate à l'étranger, des communications de données peuvent être admises à titre exceptionnel, à savoir quand les instruments juridiquement contraignants et applicables prévoient des garanties appropriées pour protéger correctement les données à l'étranger, quand la personne concernée consent au transfert, quand la communication est indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice, ou quand la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers.

Concrètement, il serait envisageable que des CSPs communiquent des données personnelles aux autorités américaines de poursuite pénale dès lors que cela serait indispensable pour sauvegarder les intérêts vitaux de la personne concernée elle-même, ou pour défendre des droits en justice dans le cadre de procédures pénales concrètes en cours. En outre, des CSPs pourraient aussi invoquer des intérêts étrangers en matière de sécurité pour faire valoir un intérêt public du point de vue de la Suisse. Mais dans tous les cas, les intérêts concernés doivent être soigneusement mis en balance. Étant donné que par principe, il faut supposer que les droits de la personnalité des personnes dont les données personnelles ont été communiquées aux autorités américaines de poursuite pénale sur la base d'injonctions de production sont gravement menacés, ces situations exceptionnelles ne devraient être acceptées comme motifs justifiant de telles communications de données que dans de très rares cas.

5.5.2.5 Autres aspects problématiques du point de vue de la protection des données et de la protection des droits fondamentaux

On peut mentionner encore d'autres aspects problématiques du point de vue de la protection des données et de la protection des droits fondamentaux en lien avec de tels traitements de données. Au regard de la protection de la sphère privée (art. 13 Cst.), ces traitements de données doivent être considérés comme sensibles à divers égards. L'art. 8 de la Convention

européenne des droits de l'homme (CEDH)[122] reconnaît le droit fondamental au respect de la vie privée. Selon la jurisprudence de la Cour européenne des droits de l'homme (CourEDH), toute ingérence dans la vie privée doit être prévue par la loi, poursuivre un but légitime et se limiter au nécessaire dans une société démocratique[123]. En rapport avec le droit à la protection des données, la Cour utilise le critère de la « stricte nécessité »[124]. Tant la CourEDH (appliquant en cela la CEDH) que la CJUE (appliquant en cela la Charte européenne) ont créé de nombreuses garanties relatives au contrôle des communications électroniques par les gouvernements[125].

Sous cet angle aussi, les aspects du *CLOUD Act* déjà évoqués au point 5.5.1.1 en rapport avec leur compatibilité au RGPD semblent problématiques[126]. Il s'agit de la réglementation différente prévue par le *CLOUD Act* concernant les données liées ou non liées au contenu, et concernant les données des « *US Persons* » et des autres personnes ; de l'absence de distinction entre le responsable du traitement et le sous-traitant ; de la surveillance en temps réel du contenu des communications ; de l'absence de droits de la personne concernée, notamment le droit d'accès et d'information ; et de l'absence de voies de recours administratives et judiciaires pour la personne concernée. L'absence de droit à un jugement par un tribunal, déjà problématique au regard des prescriptions en matière de protection des données, est en outre incompatible, notamment, avec la garantie de l'accès au juge prévue par l'art. 29*a* Cst., selon lequel toute personne a droit à ce que sa cause soit jugée par une autorité judiciaire (en Suisse)[127].

5.5.2.6 Conclusion sur la compatibilité d'un *executive agreement* avec la protection des données

Dans l'ensemble, les communications et les traitements de données effectués sur la base d'injonctions de production doivent être considérés comme fondamentalement problématiques au regard non seulement de leur compatibilité avec le RGPD, mais aussi avec le droit suisse de la protection des données, et plus généralement du point de vue des droits fondamentaux. Enfin, une condition importante pour que le caractère adéquat du niveau de protection des données assuré par la Suisse soit reconnu par la Commission européenne est la ratification du Protocole d'amendement à la Convention sur la protection des données personnelles du Conseil de l'Europe (« Convention 108+ »)[128]. La mise en œuvre, exigée par la Convention 108+, des mesures de protection des données prescrites étant une condition de sa ratification (art. 4, al. 2 Convention 108+), la conclusion d'un *executive agreement* doit être qualifiée de problématique à la lumière aussi de cette circonstance.

La protection des données n'étant pas suffisante aux USA, on peut poser pour acquis que des communications de données aux autorités américaines de poursuite pénale représenteraient une grave atteinte aux droits de la personnalité des personnes concernées. Sous réserve d'examen plus approfondi, on peut supposer que leur éventuel consentement ne représenterait probablement pas un motif justificatif valable. Il serait envisageable, certes,

---

[122] RS **0.101**

[123] Par exemple CourEDH, *Affaire Liberty et autres c. Royaume-Uni*, arrêt du 1er juillet 2008, requête 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300.

[124] CourEDH, *Szabó et Vissy c. Hongrie*, arrêt du 12 janvier 2016, requête 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814, p. 33 ; CJUE, *Digital Rights Ireland et Seitlinger e. a.*

[125] CourEDH, *Roman Zakharov c. Russie*, arrêt du 4 décembre 2015, requête 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

[126] Voir le document « Évaluation du CCBE de la loi CLOUD Act des USA » du 28.02.2019, Conseil des Barreaux Européens, contenu disponible sur : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.

[127] Voir à ce sujet les explications figurant plus bas, point 5.6.1.

[128] RS **0.235.1**

qu'un CSP puisse justifier un transfert de données par les intérêts sécuritaires des USA. Un autre motif justificatif envisageable serait que la communication soit effectuée dans l'intérêt de la personne concernée elle-même (c'est-à-dire pour sauvegarder ses intérêts vitaux ou pour défendre ses droits en justice dans le cadre d'une procédure pénale concrète). Mais même dans ce cas, lors de la pesée des intérêts, le fait que la communication de données menace gravement la personnalité des personnes concernées devrait peser lourd dans la balance.

Au regard des principes de protection des données que sont la transparence et la proportionnalité, notamment, les traitements de données effectués sur la base d'injonctions de production doivent être considérés comme problématiques. Même si, ici aussi, on ne pourrait exclure dans certains cas que les CSPs puissent invoquer un intérêt public digne de protection, ou les intérêts de la personne concernée elle-même, on peut s'attendre à ce qu'une violation des principes de protection des données, qui doit être considérée comme une atteinte grave aux droits de la personnalité de la personne concernée, ne puisse être justifiée que dans de très rares cas, conformément à la jurisprudence du Tribunal fédéral et à la position des autorités européennes de protection des données.

Même du point de vue d'autres exigences importantes pour la protection des données et la protection des droits fondamentaux, les traitements de données effectués sur la base d'injonctions de production se révèlent préoccupants. L'absence, dans le *CLOUD Act*, de droits d'accès, de rectification et de suppression des données de la personne concernée, pèse fortement dans la balance, de même que l'absence de possibilités de recours judiciaire et l'absence de garanties procédurales. Au regard notamment de la garantie de l'accès au juge prévue par l'art. 29*a* Cst., un *executive agreement* pose problème en droit suisse.

5.5.3 Quelle protection devrait être incluse dans un *executive agreement* avec les USA ?

Un éventuel *executive agreement* serait un accord international conclu entre la Suisse et les USA. Cet accord devrait comporter des garanties suffisantes pour que les standards de protection des données et de protection des droits fondamentaux correspondants au droit suisse soient garantis, y compris pour les données personnelles devant être communiquées aux autorités américaines de poursuite pénale. Faute de garanties correspondantes dans le *CLOUD Act*, les garanties et principes essentiels ainsi que les droits des personnes concernées devraient être réglés dans l'accord lui-même.

Ceci étant, on peut se demander si le cadre prescrit par le *CLOUD Act* pour les *executive agreements* permet d'offrir de telles garanties globales en matière de protection des données, notamment parce que cette loi elle-même pose des problèmes du point de vue de la protection des données. Il faut en particulier évoquer le fait que même s'il existait un tel *executive agreement*, une personne concernée n'aurait pas la possibilité de s'opposer à la communication de ses données personnelles puisque le seul mécanisme d'opposition prévu par le *CLOUD Act* ne concerne que les CSPs, et qu'il est d'ailleurs extrêmement limité. Les négociations en cours entre l'UE et les USA (voir le chiffre 4.2.2) témoignent de l'intention de l'UE de régler les échanges de preuves électroniques en matière pénale par un accord-cadre global dont la substance irait bien au-delà de celle d'un *executive agreement*.

La décision de la Commission européenne du 28 juin 2021 concernant le caractère adéquat du niveau de protection des données personnelles assuré par le Royaume-Uni selon le RGPD montre que la conclusion d'un *executive agreement* avec les USA aura des conséquences sur l'évaluation future du caractère adéquat de la protection des données assurée par la Suisse. La décision du Parlement européen du 21 mai 2021 de rejeter la décision

d'adéquation concernant le Royaume-Uni présentée par la Commission (décision motivée, entre autres, par la référence aux « onward transfers of data to other countries and bulk access to data by law enforcement »[129]) révèle le bien-fondé de cette supposition.

À la différence du Royaume-Uni, qui contrairement à la Suisse applique intégralement le RGPD, hormis dans le domaine du contrôle de l'immigration, et qui promet d'imposer dans l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act* une référence aux droits et garanties figurant dans l'accord-cadre entre l'UE et les USA, il faut supposer qu'un *executive agreement* que la Suisse conclurait avec les USA dans le cadre étroit du *CLOUD Act* ne suffirait pas à garantir le niveau de protection adéquat que l'UE exige. À cet égard, et en conformité avec les négociations entre l'UE et les USA, il faudrait plutôt viser un accord global qui règlerait intégralement les traitements et les communications de preuves électroniques en matière pénale par les CSPs aux autorités américaines et suisses de poursuite pénale, et garantirait un niveau élevé de protection des données personnelles traitées dans ce cadre et des libertés et droits fondamentaux des personnes concernées. Compte tenu de ce qui précède, il est dans l'intérêt de la Suisse d'attendre les résultats des négociations entre l'UE et les USA sur le futur accord.

Par ailleurs, il convient de suivre les évolutions actuelles au niveau européen dans le domaine de la protection des données. Dans son arrêt du 16 juillet 2020 concernant l'affaire « Schrems II », la CJUE note que les dispositions relatives aux programmes de surveillance n'offrent, dans le droit américain, pas de garanties suffisantes de respect des exigences du RGPD en matière de protection des données, ni de possibilités de recours suffisantes pour les personnes concernées qui ne sont pas américaines[130]. Dans ses décisions concernant le caractère adéquat du niveau de protection des données assuré par le Royaume-Uni, la Commission européenne s'appuie pour l'essentiel sur cette décision. De ce fait, il est probable qu'elle ait une influence majeure sur l'appréciation d'un éventuel *agreement* avec les USA sous l'angle de l'adéquation du niveau de protection des données assuré par la Suisse. De même, la mise en conformité des actes juridiques européens régissant les traitements de données dans le domaine des poursuites pénales et de l'exécution des peines avec la directive (UE) 2016/680 permet de supposer qu'à l'avenir, les communications de données depuis l'UE vers des pays tiers seront évaluées selon des critères encore plus stricts[131].

5.6 Compatibilité avec le droit suisse d'entraide judiciaire

L'entraide internationale en matière pénale (entraide judiciaire accessoire) entre la Suisse et les USA est essentiellement régie par le TEJUS, ainsi que par la loi fédérale du 3 octobre 1975 relative à ce traité (LTEJUS)[132]. Les aspects non réglementés dans le TEJUS et la LTEJUS sont couverts par l'EIMP et son ordonnance d'application (OEIMP)[133], tandis que le code de procédure pénale (CPP)[134] s'applique aux mesures dont ne traite pas directement l'EIMP. Par ailleurs, les CSPs suisses sont soumis à la LSCPT.

[129] Voir le communiqué de presse du Parlement européen du 21.5.2021, consultable à l'adresse : https://www.europarl.europa.eu/news/en/press-room/20210517IPR04124/data-protection-meps-urge-the-commission-to-amend-uk-adequacy-decisions (version du 26.5.2021).

[130] CJUE, *Schrems II,* consid. 175-178.

[131] Communication de la Commission au Parlement européen et au Conseil - Marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données, consultable à l'adresse : https://ec.europa.eu/info/sites/default/files/1_fr_act_part1_v1_0.pdf (version du 1er.7.2020).

[132] RS **351.93**

[133] RS **351.11**

[134] RS **312.0**

Il convient donc d'examiner la compatibilité du *CLOUD Act* et d'un éventuel *executive agreement* avec les bases légales précitées, sachant que l'ensemble des mesures déployées en matière de preuves électroniques bousculent clairement le cadre traditionnel de l'entraide judiciaire. Au vu des textes juridiques, cela est inévitable et tout à fait intentionnel. Cette partie explicitera néanmoins ce « changement de paradigme » – qui s'éloigne de l'entraide classique pour s'orienter vers une forme de coopération plus directe – sous l'angle des principes du droit suisse de l'entraide judiciaire et s'attachera à déterminer les possibilités et les limites qui ressortent de ces principes.

5.6.1 Motifs de refus d'une requête d'entraide judiciaire et garantie de recours judiciaire

La procédure d'entraide judiciaire suisse soumet la recevabilité des requêtes émanant d'un gouvernement étranger à certaines conditions. Les autorités doivent d'office vérifier si elles sont remplies lorsque la recherche des preuves a lieu en Suisse, et les personnes concernées peuvent s'en prévaloir dans le cadre d'une procédure devant les autorités et les tribunaux suisses. Les principaux motifs d'irrecevabilité des requêtes d'entraide judiciaire sont énumérés aux art. 2 et 3 EIMP[135]. Ainsi, aucune entraide n'est accordée pour les délits à caractère politique, militaire, fiscal[136], monétaire, commercial ou économique. Il en va de même lorsque les requêtes étrangères enfreignent les principes de procédure élémentaires et présentent de graves défauts. C'est par exemple le cas lorsque la procédure à l'étranger n'est pas conforme aux principes de la CEDH, lorsqu'elle tend à punir la personne poursuivie en raison de ses opinions politiques, de son appartenance à un groupe social déterminé, de sa race, de sa confession ou de sa nationalité, ou lorsque l'entraide risque d'aggraver la situation de la personne poursuivie pour l'une ou l'autre des raisons évoquées.

Les motifs d'irrecevabilité se fondent sur l'art. 5 Cst., qui dispose que l'activité de l'État doit toujours être conforme au droit, y compris au droit international. Un *executive agreement* autoriserait un CSP domicilié en Suisse à participer directement à une procédure pénale engagée par l'administration américaine ; les informations et les preuves (numériques) ne seraient plus collectées par l'administration suisse dans le cadre d'une procédure administrative suisse. En fournissant des données relatives à des personnes tierces (ses clients) dans le cadre d'une procédure pénale étrangère susceptible de les utiliser comme preuves, le CSP accomplirait de facto une tâche régalienne. L'*executive agreement* délèguerait donc à une personne privée, le CSP, une tâche relevant en droit suisse de la souveraineté nationale. De ce fait, le CSP resterait lié par les droits fondamentaux. Par conséquent, un *executive agreement* ne devrait pas porter atteinte au niveau de protection garanti par les libertés fondamentales, lequel correspond au niveau de protection prévu par le droit d'entraide actuel.

La Suisse devrait donc impérativement mettre en place une procédure nouvelle et directe, qui permette de faire valoir ces motifs de refus dans le cadre du *CLOUD Act.* Il ne s'agit rien de moins que de garantir l'ordre public[137], notamment pour les délits politiques et fiscaux. Les motifs de refus devraient probablement aussi être inscrits dans un éventuel *executive agreement* entre la Suisse et les USA. La Suisse devant également être en mesure de respecter les garanties minimales prévues par la CEDH, celles-ci devraient donc aussi figurer en détail dans l'*executive agreement*.

[135] Ces motifs figurent également dans les traités bilatéraux d'entraide judiciaire récents signés par la Suisse, ainsi que dans la clause d'exclusion discrétionnaire de l'ancienne version du TEJUS, dont la rédaction volontairement non explicite évoque « d'importants intérêts de nature similaire » (art. 3, al. 1, let. a).

[136] Sauf, par exception, dans les cas d'escroquerie fiscale, cf. art. 3, al. 3, EIMP.

[137] ZIMMERMANN, ch. marg. 612.

Dès lors, il se pose la question de savoir quelle procédure permettrait de garantir ces motifs de refus, car le *CLOUD Act* n'accorde aucune compétence aux autorités suisses, ni ne s'appuie sur une procédure suisse. Seul le CSP dispose de voies de recours contre la procédure américaine, devant un tribunal américain, et peut contester l'utilisation des données s'il estime qu'elle enfreint les lois suisses en vigueur. La Suisse n'a encore jamais accepté une allégeance aussi inconditionnelle à une législation ou à des tribunaux étrangers. Par ailleurs, la conformité constitutionnelle d'une procédure de cette nature, résultant d'un *executive agreement*, est très hypothétique, surtout au regard de la garantie de l'accès au juge prévue par l'art. 29*a* Cst. Un cadre d'une autre nature que celui prévu par un *executive agreement* assujetti au *CLOUD Act* serait donc très probablement nécessaire, comme évoqué dans la partie sur la protection des données.

5.6.2 Principe de la double incrimination

Le principe de la double incrimination autorise le recours à une mesure de contrainte pour satisfaire à l'obligation d'entraide judiciaire entre pays à la condition que les faits commis soient passibles de poursuites pénales aussi bien dans l'État requérant que dans l'État coopérant. Or le *CLOUD Act* ne prévoit aucune mesure de contrainte. La notion de *serious crime* définie dans l'*executive agreement* signé par le Royaume-Uni et les USA sur la base de la peine privative de liberté encourue est censée limiter la coopération sur la base du *CLOUD Act* aux délits le plus graves, mais l'accord en question ne subordonne pas l'entraide judiciaire au principe de la double incrimination. Des voix se sont élevées à plusieurs reprises pour critiquer ce point[138], car, cela signifie que tout délit punissable d'au moins trois ans de prison aux USA peut donner lieu à une injonction de production à l'intention d'un CSP domicilié au Royaume-Uni, et que ce dernier a l'obligation d'y répondre même si le délit en question n'est pas passible de sanctions pénales au Royaume-Uni. Dans le cadre d'un éventuel *executive agreement*, ce point pourrait se révéler particulièrement délicat pour la Suisse, notamment en matière de délit fiscal.

Compte tenu du principe connu de la double incrimination en matière de coopération internationale, il se pose la question de savoir si la Suisse pourrait, sur la base du *CLOUD Act*, envisager de répondre à une requête d'entraide judiciaire pour des faits ne présentant aucun caractère pénal sur son territoire. Si la réponse est négative, il faudrait ajouter le critère de la double incrimination à la notion de *serious crime* (infraction grave) dans l'*executive agreement*. Ce qui, de nouveau, ferait resurgir la question de savoir comment la conformité à ces conditions pourrait être vérifiée en l'absence de toute procédure suisse et, au besoin, de savoir comment elle pourrait être imposée. Le fait de savoir s'il suffit ou pas que le CSP – qui, rappelons-le, n'est pas la personne faisant l'objet de l'enquête – pourrait faire valoir dans une procédure pénale aux USA le fait que le délit fiscal incriminé ne rentre pas dans le champ d'application de l'entraide judiciaire en Suisse est une question de nature politique.

5.6.3 Droit d'être entendu

La question du droit à être entendu renvoie elle aussi à la Constitution dans la mesure où l'art. 29, al. 2 Cst. garantit aux parties le droit d'être entendues. Toute personne a donc le droit de présenter ses arguments, d'avoir accès à son dossier, de fournir ou de demander des preuves sur des faits susceptibles d'influer sur la décision finale, d'être associée à l'obtention desdites preuves, ainsi que de les consulter et de prendre position à leur égard pour empêcher qu'une décision lui portant injustement préjudice ne soit prise.

[138] Celle de l'ONG Human Rights Watch par exemple, dont la lettre ouverte est disponible sur Internet: https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement.

En matière de coopération pénale internationale, ces obligations résultent des art. 29 ss PA ainsi que de certaines dispositions spécifiques de l'EIMP et de la LTEJUS.

L'actuelle procédure d'entraide judiciaire avec les USA prévoit que la personne mise en cause a le droit de se faire assister d'un mandataire (art. 21 EIMP), de consulter les pièces de son dossier (art. 26 et 27 PA par référence à l'art. 9 LTEJUS) et de participer à l'exécution de la demande (art. 12, al. 2 et art. 18, al. 1 TEJUS), le droit de toute personne personnellement et directement touchée par une mesure d'entraide et ayant un intérêt digne de protection à ce qu'elle soit annulée ou modifiée de se voir notifier une décision motivée lui permettant de faire valoir son droit de recours (art. 17 s. LTEJUS) ainsi que le droit d'être informée sur lesdites voies de recours (art. 22 EIMP).

Le *CLOUD Act* permettrait à l'autorité compétente en Suisse (définie dans l'*executive agreement*) de demander directement aux CSPs ayant leur siège aux USA des informations et des données enregistrées sur leurs serveurs et, inversement, les autorités américaines pourraient directement demander aux CSPs ayant leur siège en Suisse des données stockées sur leurs serveurs. Ce système aboutirait à une situation où ni les personnes (physiques et morales) dont les données seraient requises, ni une autre autorité (par exemple l'OFJ en tant qu'autorité de surveillance ou autorité centrale), ne se verraient averties du transfert de données et informations. Elles ne pourraient donc pas demander activement à être prévenues du transfert de leurs données[139] ni s'exprimer à propos dudit transfert. Par conséquent, le droit d'être entendu de la personne ou de l'autorité directement concernée par la divulgation d'informations ne pourrait pas être garanti.

Le *CLOUD Act* ne reconnaissant pas le droit d'être entendu de la personne ou de l'autorité concernée, il convient de se demander si ce droit pourrait être inscrit dans un *executive agreement*. Dans le cas d'une réponse positive, il faut de nouveau se poser la question de savoir si ce droit pourrait être garanti en l'absence de toute procédure en Suisse. Dès lors, un *executive agreement* serait difficilement compatible avec l'exigence constitutionnelle posée par l'art. 29., al. 2 Cst. Le cadre du traité devrait donc être élargi.

5.6.4 Autorité de surveillance et de contrôle

L'OFJ est, au premier chef, l'autorité chargée de l'exécution des traités et de la législation fédérale en matière de coopération pénale internationale (art. 17, al. 2 EIMP et art. 7, al. 6a de l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police, Org DFJP)[140]. Dans le domaine de l'entraide pénale internationale avec les USA, il exerce à la fois la fonction d'autorité centrale instituée par l'art. 28, al. 1 TEJUS et la fonction d'autorité de surveillance qui lui revient (art. 19, al. 1, première phrase LTEJUS) en raison de sa qualité pour recourir contre les décisions de l'autorité cantonale ou fédérale d'exécution. Il est également fondé à recourir devant le Tribunal fédéral contre les décisions du Tribunal pénal fédéral (art. 19, al. 1, première phrase LTEJUS).

En plus de la possibilité de déposer un recours, l'OFJ exerce son devoir de surveillance sur toute la procédure d'entraide en Suisse, notamment lorsqu'il vérifie si les conditions de recevabilité d'une requête d'entraide sont remplies, si les décisions prises par les autorités d'exécution (notamment les ministères publics cantonaux et le Ministère public de la Confédération) respectent les dispositions du droit d'entraide et lorsqu'il transmet les informations et les

[139] En vertu de l'art. 3, al. 1, let. a, ch. 3 de la loi fédérale sur le principe de la transparence dans l'administration (LTrans, RS **152.3**), les procédures d'entraide judiciaire et administrative internationale sont exclues du champ d'application de la loi. L'accès aux documents relèverait donc des seules dispositions de l'*executive agreement*.

[140] RS **172.213.1**

moyens de preuve en précisant l'emploi qui peut en être fait par l'autorité requérante selon le principe de spécialité (art. 5 TEJU). L'OFJ contrôle également les requêtes d'entraide adressées aux États étrangers (art. 30 EIMP).

Le *CLOUD Act* permet aux autorités suisses désignées de demander directement des données aux CSPs américains, et aux autorités américaines de faire de même avec les CSPs suisses. Les CSPs suisses recevraient ainsi des injonctions de production dont l'OFJ n'aurait très probablement pas connaissance et sur lesquels il ne serait donc pas à même d'exercer son devoir de surveillance. En outre, l'autorité définie dans l'*executive agreement* comme autorité compétente pour établir des injonctions de production en Suisse serait toute à la fois autorité d'exécution et seule garante du respect du droit.

Le *CLOUD Act* attribue aux CSPs un rôle clé pour les requêtes déposées par les USA. Ils seraient seuls à avoir connaissance d'une demande et auraient le contrôle sur la procédure en découlant[141]. Les prestataires de petite taille pourraient manquer d'expertise et de ressources pour assumer ce rôle[142]. Pour les requêtes déposées par la Suisse, ce rôle serait endossé par les autorités d'exécution.

Bien qu'une injonction de production soit censée être soumise à un certain contrôle[143], le *CLOUD Act* ne semble pas prévoir l'institution d'une autorité de surveillance en tant que telle. L'un de ses buts semblant être l'immédiateté et la rapidité de l'échange d'informations et de données, un mécanisme de surveillance ralentirait effectivement le processus. Toutefois, la possibilité d'instaurer un mécanisme de contrôle limité dans un *executive agreement* ne semble pas exclue, comme le montre l'accord conclu entre le Royaume-Uni et les USA. (cf. ci-dessus chiffre 4.1).

Il convient donc de se demander si – contrairement au concept du *CLOUD Act* – une autorité de surveillance ou de contrôle pourrait être instituée dans le cadre d'un *executive agreement*, tant pour les requêtes d'entraide adressées à la Suisse que pour celles qu'elle dépose. Cela serait probablement la seule façon de garantir la constitutionnalité de l'entraide internationale (cf. ci-dessous chiffre 5.6.8.). Reste à définir la place que tiendrait cette autorité de surveillance, ainsi que les rôles et les possibilités concrètes de contrôle qui seraient les siens.

5.6.5 Principe de spécialité

Dans le domaine de l'entraide, le principe de spécialité interdit l'utilisation par l'État requérant des documents, renseignements et informations reçus dans une procédure visant des délits pour lesquels l'entraide est exclue en Suisse. Cela concerne les infractions politiques, militaires, fiscaux[144], monétaires et économiques ou les cas dans lesquels l'octroi de la coopération compromettrait la souveraineté, la sûreté, l'ordre public ou d'autres intérêts essentiels de l'État à qui la requête est adressée[145]. Le principe de spécialité protège aussi bien la souveraineté de la Suisse que la personne visée par les actes d'entraide. Le principe de spécialité s'impose à l'État requérant, ainsi qu'à tout État tiers qui pourrait avoir ultérieurement connaissance des renseignements par son entremise.

---

[141] Cf. BISMUTH, p. 685.

[142] BISMUTH, p. 685.

[143] *CLOUD Act*, § 2523 (b) (3) (D) (v).

[144] L'entraide est autorisée pour les escroqueries fiscales, cf. art. 3, al. 3 EIMP.

[145] Cf. l'art. 2 de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 (CEEJ, RS **0.351.1**) ainsi que l'art. 1*a* et l'art. 3 EIMP.

Le principe de spécialité s'applique aussi aux relations avec les USA[146]. Même si les entités gouvernementales fondées par un *executive agreement* à demander des données au sens de l'accord devaient avoir un mandat clairement défini juridiquement ainsi que des procédures transparentes, notamment en ce qui concerne l'utilisation des données[147], le *CLOUD Act* ne semble contenir aucune clause s'apparentant au « principe de spécialité », ou du moins aucune réglementation claire et effective qui autoriserait ou interdirait l'utilisation des données reçues.

L'accord entre le Royaume-Uni et les USA reprend une possibilité déjà prévue dans le *CLOUD Act*: les données obtenues sur la base de l'accord ne peuvent être transmises à un État tiers sans le consentement de l'État dans lequel le CSP a son siège (art. 8, al. 2). L'accord prévoit également que l'État tiers doit être informé lorsque la personne dont les informations sont demandées ne se trouve pas au Royaume-Uni ou n'est pas un ressortissant américain[148]. Si les données concernent des crimes qui pourraient mener à la peine de mort aux USA ou à la violation de la liberté d'expression au Royaume-Uni, l'autorité centrale de l'autre État doit être informée et donner son accord (art. 8, al. 4). Comme mentionné au point 4.1, les données obtenues sur la base du *CLOUD Act* ne peuvent être utilisées pour prononcer une peine de mort aux USA ou pour violer la liberté d'expression au Royaume-Uni sans l'accord préalable de l'autre État. Le Royaume-Uni a donc un droit de veto en ce qui concerne l'utilisation des preuves obtenues dans les affaires où la peine de mort est requise.

Dans le cadre d'un *executive agreement*, le contrôle de l'utilisation des données transmises échapperait largement à la Suisse, et plus encore si aucune autorité de surveillance puissante (au sens large) n'était instituée par cet accord. La question se pose donc de savoir si le principe de spécialité tel qu'il est pratiqué aujourd'hui (avec l'exception des délits fiscaux par exemple) pourrait être inscrit dans un *executive agreement*. Mais avant tout, il faut s'interroger sur ses modalités d'application : comment les définir pour qu'elles soient suffisamment conciliables avec les règles de droit suisse de rang supérieur, et de surcroît dans une procédure exclusivement américaine et où la seule partie appliquant ces règles serait le CSP concerné ?

5.6.6 Limitation de la coopération internationale pour motifs politiques

Il a été mentionné plus haut que la Suisse pouvait refuser l'entraide judiciaire si la demande était susceptible de porter atteinte à la souveraineté, à la sûreté, à l'ordre public ou à d'autres intérêts essentiels de l'État[149]. Généralement, une telle situation survient à la suite d'une réclamation de la partie concernée. Lorsque de tels intérêts sont en jeu, l'entraide judiciaire peut également être assortie de conditions[150]. Dans ce cas, la décision relève de la compétence du DFJP, qui prend l'avis des autres départements. La décision du DFJP peut donner lieu à un recours au Conseil fédéral. Une telle « clause de protection de la souveraineté » serait difficilement compatible avec le *CLOUD Act*.

[146] Cf. art. 5, al. 1 TEJUS et art. 67 EIMP. Pour les réserves, cf. ZIMMERMANN, ch. marg. 734 avec commentaires supplémentaires.

[147] *CLOUD Act*, § 2523 (b) (1) (B) (iv)

[148] Art. 5 de l'accord. Cf. également DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards » ; dans ce contexte, l'État tiers est l'État dont la personne concernée possède la nationalité.

[149] Art. 1a EIMP ; cf. aussi art. 3, al. 1, let. a TEJUS.

[150] ZIMMERMANN, ch. marg. 714.

5.6.7 Compatibilité avec le code de procédure pénale et la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

La rédaction des dispositions d'un éventuel accord bilatéral devrait également se conformer aux règles en vigueur du CPP[151] et des actes législatifs en matière de procédure pénale, ainsi qu'à la LSCPT[152]. Il faudrait impérativement veiller à ce que les autorités étrangères ne se voient pas accorder des pouvoirs et des possibilités plus étendus que les autorités nationales. Cela signifie par exemple que les autorités américaines de poursuite pénale ne pourraient pas émettre d'injonctions de production (transfrontières) de plus large portée que les autorités pénales suisses vis-à-vis des CSPs domiciliés en Suisse, ou que la protection légale concernant les injonctions de production américaines ne devrait pas être moindre que celle qui concerne les mesures nationales[153].

Au vu du système mis en place par le *CLOUD Act*, cet impératif ne va pas sans difficultés. Les exigences du CPP et de la LSCPT devraient s'appliquer dans les procédures américaines, y compris pour les découvertes fortuites (art. 243 et 278 CPP), l'interdiction d'exploiter les preuves, etc., car il n'y aurait plus de procédure suisse.

La procédure inscrite dans le *CLOUD Act* pourrait difficilement être réglementée dans un *executive agreement* d'une manière qui correspondrait en Suisse aux bases légales précitées. Si une autorité suisse assumait une fonction de surveillance en tant qu'autorité centrale pour la collecte de données par les USA, elle effectuerait un contrôle préliminaire et pourrait rappeler le principe de spécialité lors de l'envoi des données. Mais même ainsi le respect des exigences aux procédures nationales ne serait pas garanti. Il est ainsi difficilement envisageable qu'un droit de recours suffisamment large puisse être instauré dans ce cadre.

Dès lors, il convient de se demander si les principales dispositions en vigueur afférentes à la transmission transfrontière de preuves électroniques ne devraient pas plutôt faire l'objet d'une loi nationale. Une telle loi pourrait servir de base légale pour un nombre infini d'accords bilatéraux. C'est la voie adoptée par le Royaume-Uni et l'Australie. Un tel système permettrait d'instaurer un socle de compatibilité par voie législative, mais laisserait tout de même subsister des questions de droit pour l'*executive agreement* qui serait conclu sur sa base. Il faudrait ainsi commencer par définir les liens concrets entre les différents ordres juridiques et, en plus, préciser toute une série d'aspects techniques, comme la question des délais de conservation des données secondaires ou leur application aux CSPs américains. Le droit suisse prévoit par exemple un délai de conservation ainsi qu'une durée pour la surveillance rétroactive, ce qui ne semble pas être le cas des USA. Qu'en serait-il dans l'accord bilatéral ?

---

[151] Principales conditions posées par le CP pour la surveillance de la correspondance par poste et télécommunication : ordonnance de la surveillance par le ministère public (art. 269, al. 1, phrase introductive ; art. 273, al. 1 CPP) ; graves soupçons laissant présumer une des infractions énumérées à l'art. 269, al. 2 CPP pour la surveillance du contenu des télécommunications (art. 269, al. 1, let. a CPP) ou un crime, un délit ou une contravention au sens de l'art. 179^{septies} CP pour la surveillance des données secondaires (art. 273, al. 1 CPP) ; gravité de l'infraction justifiant la surveillance (respect du principe de la proportionnalité : art. 269, al. 1, let. b. CPP) ; respect du principe de la subsidiarité (art. 269, al. 1, let. c CPP) ; autorisation par le tribunal des mesures de contrainte (art. 272, al. 1 et art. 273, al. 2 CPP) ; gestion des informations non nécessaires (art. 276 CPP) ; recevabilité des informations recueillies lors d'une surveillance non autorisée (art. 277 CPP) ; règles pour les découvertes fortuites (art. 278 CPP) ; communication de la surveillance (art. 279, al. 1 et 2 CPP) ; recours (art. 279, al. 3 CPP).

[152] Les principales conditions posées par de la LSCPT pour la surveillance de la correspondance par poste et télécommunication sont: le service chargé de la surveillance de la correspondance par poste et télécommunication constitue pour ainsi dire l'interface entre les autorités de poursuite pénale et l'opérateur (l'injonction de surveiller n'est pas directement communiquée par les autorités pénales à l'opérateur ; elle est d'abord transmise au Service SCPT qui le transmet lui-même à l'opérateur en vertu d'une décision y afférente [art. 5 PA] ; les données communiquées par l'opérateur ne sont pas directement transmises aux autorités de poursuite pénale, mais au Service SCPT, qui ensuite les communique au service pénale compétent ; obligations spécifiques de différentes catégories d'opérateurs, citées dans la loi ou les ordonnances y relatives, obligations plus ou moins larges selon la nature de l'opérateur ; rémunération de l'opérateur pour chaque surveillance versée par le Service SCPT et financé en partie par ledit service et en partie par l'autorité de poursuite pénale ; recours de l'opérateur contre la décision administrative du Service SCPT (aucune réclamation ne peut être déposée dans le cadre d'une procédure de droit pénal).

[153] Cf. p. ex. art. 274 et 279 CPP.

5.6.8 Quels contenus « juridiques d'entraide judiciaire » devraient figurer dans un *executive agreement* ?

Même si la Suisse concluait un *executive agreement,* elle resterait soumise à ses obligations en matière de droits humains et de libertés fondamentales. Du point de vue juridique, il faudrait donc impérativement trouver les moyens de garantir le respect des droits constitutionnels tels que le *droit d'être entendu* (art. 29, al. 2 Cst.) et la *garantie de l'accès au juge* (art. 29*a* Cst.). Le respect des *garanties minimales de la CEDH* ainsi que de l'ordre public suisse (notamment en cas d'exclusion de l'entraide judiciaire dans le domaine des délits politiques ou fiscaux) doit également être garanti. Il faut également s'assurer qu'un éventuel *executive agreement* ne privilégie pas de manière exagérée les autorités de poursuite pénale américaines par rapport aux autorités de poursuite pénale suisses, en ce qui concerne la collecte des données en Suisse (cf. point 5.4.3.). Il est difficile d'imaginer comment toutes les dispositions du *code de procédure pénale suisse* pourraient être ancrées dans un *executive agreement*. Il est donc indispensable que la Suisse définisse d'abord ses propres standards en matière de production transfrontière de preuves électroniques (système *e-evidence)*, avant de coopérer dans ce domaine avec les États partenaires dans le cadre de traités. En outre, cela permettrait de concevoir ce système de manière autonome et en tenant compte du droit suisse, de sorte que la souveraineté de la Suisse serait suffisamment garantie et nos valeurs fondamentales préservées, même en cas de collaboration directe dans le domaine des preuves électroniques.

6 Sécurité des données et décryptage

6.1 Transmission sécurisée

Le transfert de données d'un CSP suisse vers une autorité de poursuite pénale américaine doit être conforme à la législation suisse. En l'espèce, il faut vérifier comment les données personnelles sont transférées d'un CSP à une autorité étrangère. Pour les systèmes de messageries électroniques (ou les autres avec des serveurs intermédiaires), un cryptage du contenu et du transfert est nécessaire pour garantir la protection des données pendant tout le transfert. Pour une plateforme de téléchargement (ou un système similaire sans transmission de données à d'autres systèmes), le cryptage du transfert semble suffisant si la plateforme est gérée par l'autorité elle-même. Si la plateforme de téléchargement de l'entreprise est externalisée, un cryptage du contenu est à nouveau nécessaire.

Si des données particulièrement sensibles devaient être transférées, ce qui est en général le cas dans le cadre de procédures pénales, le guide relatif aux mesures techniques et organisationnelles de la protection des données du PFPDT prévoit le cryptage permanent des données personnelles[154].

Un *executive agreement* devrait donc également contenir des dispositions qui garantissent le respect de ces règles de transmission des données à une autorité de poursuite pénale américaine. Par conséquent, les résultats des négociations entre les USA et l'UE devraient être utiles pour la Suisse.

[154] PFPDT, guide relatif aux mesures techniques et organisationnelles de la protection des données, août 2015, p. 20, disponible sur : https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html.

6.2 Cryptage neutre

La conservation des données sous une forme cryptée *chez le* CSP pose problème en ce qui concerne la question de la transmission légale et sécurisée des données d'un CSP suisse aux autorités de poursuite pénale américaines ou inversement.

Les CSPs peuvent proposer une multitude de prestations de services conformes aux exigences relatives à la sécurité des données (des clients). Les cryptages en font partie. Le *CLOUD Act* n'impose pas de décrypter les données. Il ne contient en particulier aucune disposition relative au décryptage des données dont disposent les CSPs pour le compte de leurs utilisateurs[155]. Les CSPs ne peuvent donc pas être contraints de décrypter les données qui ont été cryptées par les clients[156].

Dans des dispositions légales spéciales (p. ex. art. 12, al. 5 de l'ordonnance sur le dossier électronique du patient [ODEP])[157], la FINMA ou l'OFSP ont certes imposé la conservation des données des clients en Suisse et selon le droit suisse. Même si les personnes concernées, à savoir ici les fournisseurs de prestations financières et médicales, respectent cette obligation en conservant des données particulièrement sensibles dans des datacenters suisses, les autorités américaines peuvent avoir accès aux données dans certaines situations relevant du champ d'application du *CLOUD Act*. Lors du transfert des données, des devoirs de discrétion légaux et/ou contractuels peuvent exiger que les données soient conservées sous une forme cryptée. Lors du cryptage, il existe diverses procédures techniques qui diffèrent notamment selon qu'elles prévoient ou non la possibilité d'accéder aux données par des moyens techniques en vertu du *CLOUD Act*.

Il convient d'abord de faire une distinction entre le cryptage côté client et le cryptage côté serveur. Lorsque les données sont déjà cryptées sur l'ordinateur du client ou du propriétaire des données, puis transmises au CSP sous cette forme (cryptage côté client), la clé de chiffrement reste chez le client. Le CSP ne peut pas décrypter les données. Par conséquent, celles-ci sont protégées contre un accès des autorités américaines dans le cadre du *CLOUD Act*, sans que le client ou le propriétaire des données ait à intervenir. La situation est différente en cas de cryptage côté serveur. Il faut faire une distinction entre trois variantes. Dans la première variante, la gestion de la clé de chiffrement est confiée au CSP qui la conserve sur le cloud et y a accès de manière légale. En principe, le CSP peut permettre aux autorités américaines d'avoir accès aux données cryptées. La protection des données des clients dépend de la volonté de coopération du CSP car, tel que mentionné ci-dessus, le CSP n'est pas tenu de décrypter les données des clients conformément au *CLOUD Act*. Dans la deuxième variante, le client gère seul la clé de chiffrement (« *Bring Your Own Key*, BYOK », parfois aussi « *Bring Your Own Encryption*, BYOE »). Toutefois, celle-ci doit être enregistrée et sauvegardée sur le cloud. Cependant, la conservation de la clé de chiffrement sur le cloud permet au CSP de décrypter et de donc de produire les données en vertu du *CLOUD Act*. Qu'il y soit autorisé ou non dépend en premier lieu des conditions d'utilisation et en second lieu de la pression exercée par les autorités américaines. Dans la troisième variante, le client sauvegarde la clé de chiffrement uniquement sur son propre disque dur. Pour cette variante, la protection est la

[155] « The terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data », *CLOUD Act*, § 2523(b)(3). Voir également DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act* », p. 6 ; ZAGARIS, « U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption », p. 360.

[156] Conformément au droit suisse, les CSPs ne peuvent être contraints de décrypter que les données qu'ils ont eux-mêmes cryptées (art. 26, al. 2, let. c LSCPT).

[157] RS **816.11**

même que pour le cryptage côté client. Le CSP ne peut pas décrypter les données sans l'accord du client ou du propriétaire des données.

Dans ce contexte, ce qui suit apparaît comme une évidence: conformément au *CLOUD Act*, les CSPs ne sont pas tenus de décrypter les données dont ils disposent pour le compte de leurs utilisateurs ou clients[158]. Nonobstant cette règle ou plutôt absence de règle, il faut être conscient du fait qu'un accès des autorités américaines à ces données ne peut pas être exclu, si un moyen technique ou un accord contractuel le permet.

7 Conclusion

Un des plus grands défis à relever dans le domaine de la coopération pénale internationale est la conservation et la production des preuves électroniques. Dans ce domaine, des approches nouvelles et innovantes sont nécessaires car la procédure actuelle rend très difficile la poursuite pénale au niveau international. Le présent rapport apporte des éclaircissements sur les différentes initiatives internationales visant à faciliter l'accès aux preuves électroniques: le Conseil de l'Europe élabore actuellement un deuxième protocole pour la Convention de Budapest, l'UE est en train d'adopter une législation *e-evidence* qui prescrit des règles européennes de conservation et de production des preuves électroniques et l'ONU prépare un instrument multilatéral pour lutter contre la cybercriminalité. Parallèlement à cela, on observe des évolutions dans les différents États. La plus importante initiative nationale est l'adoption du *CLOUD Act* par les USA. Pour les autorités de poursuite pénale américaines et les CSPs, cette loi fédérale américaine a une portée extraterritoriale. Elle permet aux autorités de poursuite pénale américaines d'accéder aux données des CSPs dont le siège est aux USA, que ces données soient enregistrées aux USA ou à l'étranger. En outre, la loi vise à « internationaliser » le système américain en donnant aux autorités américaines la possibilité de conclure un *executive agreement*, afin d'étendre le système et le domaine d'application du *CLOUD Act* aux autres États. Comme les plus grands CSPs ont leur siège aux USA, la collaboration avec cet État en matière de preuves électroniques a, notamment pour la Suisse, une importance particulière. C'est pourquoi, la question de la conclusion d'un éventuel *executive agreement* avec les USA fait débat. Le présent rapport traite cette question dans le contexte étendu du « Changement de paradigme dans le domaine de l'entraide pénale » et eu égard aux divers aspects juridiques qu'elle revêt. Il examine la compatibilité entre le *CLOUD Act* et le droit suisse, en particulier dans deux domaines: le droit de la protection des données et les principes de la coopération pénale internationale. L'OFJ est arrivé aux conclusions suivantes:

- Droit de la protection des données: les données concernées par le *CLOUD Act* sont des données personnelles au sens du droit de la protection des données. Dans ce contexte, il est particulièrement important qu'en cas de conclusion d'un *executive agreement*, les termes de cet accord soient compatibles avec le droit suisse de la protection des données. Le droit européen de la protection des données n'est certes pas directement applicable en Suisse, mais il est pris en compte de manière exhaustive dans le présent rapport. En effet, la Suisse est considérée par l'UE comme un État tiers avec un niveau adéquat de protection des données (décision d'adéquation), de sorte qu'elle peut échanger des données personnelles avec les États membres de l'UE et participer au libre flux des données avec l'UE. De ce fait, elle a un accès illimité au *« marché unique numérique »* de l'UE. Par conséquent, le droit européen de la protection des données a une grande influence sur la Suisse. De plus, le droit suisse de la protection des données vient d'être entièrement révisé. Le présent rapport analyse la compatibilité du *CLOUD Act* avec les versions actuelle et future du droit de la protection des données. Il ressort de cette analyse qu'une production de

[158] DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ».

données exigée au moyen d'une injonction de production adressée sur la base du *CLOUD Act* n'est compatible avec les droit suisse et européen de la protection des données que dans des cas exceptionnels et spécifiques.

- Droit de l'entraide judiciaire: le *CLOUD Act* permet à un CSP à l'étranger de transmettre des données électroniques à une autorité de poursuite pénale américaine, qui pourra ensuite utiliser les données et informations reçues dans le cadre d'une procédure pénale. Cette collaboration directe remplacerait, du moins en partie, la voie traditionnelle de l'entraide judiciaire. La conclusion d'un *executive agreement* entraînerait donc un *changement de paradigme* dans le domaine de la coopération pénale internationale: pour la première fois, une entité privée suisse participerait directement à une procédure pénale étrangère, sans qu'une procédure suisse ou du moins une autorisation soit en l'espèce nécessaire à cet effet. Cette nouvelle forme de collaboration aurait des effets sur les différents principes et garanties qui s'appliquent en vertu du droit de l'entraide pénale internationale. Elle impacterait en particulier les garanties constitutionnelles du droit d'être entendu et de la garantie de l'accès au juge, car la personne concernée par la production de données (propriétaire des données) n'aurait plus connaissance de leur divulgation et ne pourrait donc plus s'y opposer par voie de recours. L'OFJ ne pourrait plus jouer son rôle d'autorité de surveillance dans le cadre d'une procédure d'entraide judiciaire et donc garantir le respect des principes juridiques applicables en Suisse. La production dépendrait uniquement de la volonté de coopération du CSP. Ainsi, les droits d'une personne concernée par une requête d'entraide judiciaire seraient bafoués. Il en va de même de la possibilité pour l'État de contrôler la procédure et donc de garantir au final la souveraineté de la Suisse. Eu égard à la compatibilité avec les principes du droit de l'entraide judiciaire, le *CLOUD Act* soulève donc de grandes questions et semble difficilement compatible avec le droit suisse de rang supérieur.

8 Procédure à suivre

Le présent rapport est censé servir de *base à une discussion* avec les services partenaires à l'intérieur et à l'extérieur de l'administration fédérale, ainsi qu'avec les parties prenantes de l'économie privée, des associations professionnelles et des autres groupes de personnes intéressés. Sur la base des résultats de cette discussion, l'OFJ demandera en temps voulu au Secrétariat général du DFJP de lui indiquer la procédure à suivre en ce qui concerne le US *CLOUD Act* en l'espèce et les preuves électroniques en général.

9 Bibliographie

BAERISWYL, B., « Vorbemerkungen zu Art. 4–11*a* » dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpflis Handkommentar*, Berne : Stämpfli 2015.

BAERISWYL, B., « Art. 4 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpflis Handkommentar*, Berne : Stämpfli 2015.

BAERISWYL, B., « Art. 10*a* », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpflis Handkommentar*, Berne : Stämpfli 2015.

BAERISWYL, B., BLONSKI, D., « Art. 6 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpflis Handkommentar*, Berne : Stämpfli 2015.

BILGIC, S., « Something Old, Something New, and Something Moot: The Privacy Crisis Under the *CLOUD Act* », 32:1 2018 *Harvard Journal of Law and Technology*, p. 321.

BISMUTH, R., « Le *Cloud Act* face au projet européen *E-Evidence:* confrontation ou coopération ? », dans *Revue critique de droit international privé*, 2019:3, p. 681.

CHRISTAKIS, T., « 21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement: (and an Explanation of How it Works – with Charts) », *European Law Blog*, 17.10.2019, disponible sur : https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/.

DASKAL, J., « Unpacking the *CLOUD Act* », 2018:4 *eucrim*, p. 220.

DASKAL, J., « *Microsoft Ireland*, the *CLOUD Act*, and International Lawmaking 2.0 », 2018:71 *Stanford Law Review Online* p. 9, disponible sur : Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 | Stanford Law Review.

DASKAL, J., SWIRE, P., « The UK-*US CLOUD Act* Agreement is Finally Here, Containing New Safeguards », *Just Security*, 08.10.2019, disponible sur : https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/.

DASKAL, J., SWIRE, P., CHRISTAKIS, T., « The globalization of criminal evidence », 16.10.2018, disponible sur : https://iapp.org/news/a/the-globalization-of-criminal-evidence/.

LUTZ T., EGLI L., « Braucht die Schweiz ein CLOUD Act executive agreement ? », Schweizerische Juristen-Zeitung SJZ 2021, p. 119.

MAURER-LAMBROU, U., STEINER, A., « Art. 6 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.

MAURER-LAMBROU, U., STEINER, A., « Art. 4 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.

PLENACOSTE, F., DAOUD, E., « *CLOUD Act*: Des inquiétudes légitimes », 2018:12 *Droit de la propriété intellectuelle et du numérique,* p. 680.

RAMPINI, C., « ART. 13 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.

ROSENTHAL, D., JÖHRI, Y., *Handkommentar zum Datenschutzgesetz*, Zurich : Schulthess 2008.

ROSENTHAL, D., « Mit Berufsgeheimnissen in die Cloud: So geht es trotz US *CLOUD Act* », *Jusletter*, 10 août 2020.

TSILIKIS, D., « Auf der grenzüberschreitenden Suche nach E-Evidence im Strafverfahren: die Unionsrechtsperspektive im digitalen Zeitalter », dans Meier, J., Zurkinden, N., Staffler, L. (Éditeur), *Recht und Innovation – Innovation durch Recht, im Recht und als Herausforderung für das Recht*, Zurich : Dike 2020, p. 163.

ZAGARIS, B., « U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption », 35:10 2019 *International Enforcement Law Reporter,* p. 357.

ZERDICK, T., « Art. 48 – Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung » dans Ehmann, E., Selmayr, M. (Éditeur), *Datenschutz-Grundverordnung – Kommentar*, 2e édition, Beck: Munich 2018.

ZIMMERMANN, R., *La coopération judiciaire internationale en matière pénale*, 5e édition, Berne : Stämpfli 2019.

EDPB/CEPD, « Initial legal assessment of the impact of the US *CLOUD Act* on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence », 10 juillet 2019, disponible sur : https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (EDPB/CEPD, Initial legal assessment).

US DOJ, « Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the *CLOUD Act* », White Paper, 2019, disponible sur : https://www.justice.gov/dag/page/file/1153436/download.

10 Abréviations

al.	alinéa
art.	article
FF	Feuille fédérale
LF	Loi fédérale
LTEJUS	Loi fédérale relative au traité conclu avec les États-Unis d'Amérique sur l'entraide judiciaire en matière pénale
OFJ	Office fédéral de la justice
BSK	Commentaire bâlois
let.	lettre(s)
Convention de Budapest	Convention du Conseil de l'Europe sur la cybercriminalité (Convention sur la cybercriminalité)
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
Cst.	Constitution fédérale de la Confédération suisse
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act* (USA)
CSP	Communication Service Provider – fournisseur de services de communication
Convention 108+	Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des données
Service SCPT	Service chargé de la surveillance de la correspondance par poste et télécommunication
DOJ	Département américain de la justice
LPD	Loi fédérale sur la protection des données
RGPD	Règlement général de l'UE sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
EDPB	Comité européen de la protection des données
CEPD	Contrôleur européen de la protection de données
Directive décision d'enquête européenne	Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale
Preuve électronique	Mesures de l'UE pour améliorer l'accès transfrontière aux preuves électroniques
CourEDH	Cour européenne des droits de l'homme
CEDH	Convention européenne des droits de l'homme
EPOC	Injonction européenne de production
EPOC-PR	Injonction européenne de conservation
consid.	considérant
EUeR	Convention européenne d'entraide judiciaire en matière pénale
CJUE	Cour de justice de l'Union européenne
FST	Fournisseurs de services de télécommunication
FINMA	Autorité fédérale de surveillance des marchés financiers
LTC	Loi sur les télécommunications
SG-DFJP	Secrétariat général du Département fédéral de justice et police
EIMP	Loi fédérale sur l'entraide internationale en matière pénale (loi sur l'entraide pénale internationale)
OEIMP	Ordonnance sur l'entraide internationale en matière pénale
nLPD	Révision totale de la loi sur la protection des données du 25.9.2020
Org DFJP	Ordonnance sur l'organisation du Département fédéral de justice et police
GEQ	Gouvernement étranger qualifié (État ayant signé un *executive agreement a*vec les USA)
TEJUS	Traité entre la Suisse et les Etats-Unis sur l'entraide judiciaire en matière pénale
SCA	*Stored Communications Act* (USA)
LPDS	Loi fédérale sur la protection des données dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal
STCE	Série des traités du Conseil de l'Europe

CS	Commentaire Stämpfli
RS	Recueil systématique du droit fédéral
CPJI	Cour permanente de justice internationale (dissolution en 1946)
CP	Code pénal suisse
CPP	Code de procédure pénale suisse
T-CY	Comité du Conseil de l'Europe de la Convention sur la cybercriminalité
GBR	Royaume-Uni
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
PA	Loi fédérale sur la procédure administrative
WVK	Convention de Vienne sur le droit des traités
ch.	chiffre