US CLOUD Act – un aperçu

Philipp Fischer et Sébastien Pittet, le 8 novembre 2021

Depuis son adoption en mars 2018, le *US CLOUD Act* a déjà fait couler beaucoup d'encre. La publication, le 17 septembre 2021, par l'Office fédéral de la justice d'un rapport (le « **Rapport** ») qui analyse la compatibilité du *US CLOUD Act* avec le droit suisse, en particulier la règlementation en matière de protection des données, offre l'occasion de revenir sur cette législation américaine qui semble planer comme une épée de Damoclès sur chaque projet impliquant le recours à un prestataire de services américain, tout particulièrement dans le domaine du *cloud computing* vu que les trois *market leaders* actuels (Microsoft, Amazon et Google) ont tous leur siège aux États-Unis.

I. Présentation générale du *US CLOUD Act*

Le *US CLOUD Act* est une loi fédérale américaine adoptée suite à une procédure judiciaire qui opposait les autorités américaines au Groupe Microsoft. Les autorités américaines avaient exigé de Microsoft la communication de courriels sauvegardés sur des serveurs hébergés par une société affiliée à Microsoft en Irlande. Microsoft avait refusé au motif que les informations demandées n'étaient pas conservées sur sol américain et échappaient donc à la compétence des autorités américaines. La juridiction d'appel a confirmé l'argumentation de Microsoft. Avant que la Cour Suprême des États-Unis n'ait eu l'occasion de se prononcer sur cette question, le Congrès américain a adopté le *US CLOUD Act* qui confère expressément aux autorités américaines un droit d'accès sur des données hébergées à l'étranger. Le *US CLOUD Act* complète le *Stored Communications Act* (le « **SCA** ») en vigueur depuis 1986.

Sur le plan des concepts, le *US CLOUD Act* est subdivisé en deux parties, l'une ayant trait aux obligations des entreprises concernées (cf. Section 1 ci-après) et l'autre prévoyant la possibilité de conclure des *executive agreements* entre les États-Unis et des pays tiers (cf. Section 2 ci-après).

1. US CLOUD Act – Partie 1

La première partie du *US CLOUD Act* oblige certains prestataires de services informatiques qui disposent d'un lien avec les États-Unis à transmettre des données aux autorités américaines (indépendamment du lieu d'hébergement de ces données), pour autant que la procé-

dure dans le cadre de laquelle ces données sont requises soit liée à des crimes graves (*serious crimes*). Dans ce contexte, plusieurs points méritent d'être précisés :

1. Le *US CLOUD Act* s'adresse aux fournisseurs (i) de services électroniques de communication (*electronic communication service providers*) et (ii) de services informatiques à distance (*remote computing service providers*) (ces deux types de prestataires visés seront désignés par le terme de « Prestataires IT » dans la présente note). D'une part, un fournisseur offre un *service électronique de communication* lorsqu'il donne la possibilité à ses utilisateurs d'envoyer ou de recevoir des communications électroniques. D'autre part, un fournisseur offre un *service informatique à distance* lorsqu'il propose des services de stockage ou de traitement informatique au moyen d'un système électronique de communication. Le champ d'application à raison de la matière du *US CLOUD Act* est donc large et inclut en particulier les *cloud service providers* tels qu'Amazon, Google et Microsoft.
2. Le *US CLOUD Act* concerne les Prestataires IT soumis à la juridiction américaine, à savoir principalement les entreprises incorporées aux États-Unis (pour toutes les données que ces entreprises sont réputées « contrôler »), mais potentiellement également des entreprises non-américaines qui disposent d'une filiale ou d'un autre type de présence stable sur sol américain. Il appartient aux autorités américaines de déterminer au cas par cas si une entreprise étrangère située en dehors des États-Unis est soumise à la juridiction américaine en raison de ses activités.
3. Le *US CLOUD Act* concerne les données « en possession, sous la garde ou sous le contrôle » du Prestataire IT soumis à la juridiction américaine, indépendamment de la localisation effective de ces données :

> « *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.* » (Section 2713 (a) (1) du *US CLOUD Act* / nous mettons en évidence).

4. Finalement, l'on rappellera que la Suisse est partie à un accord international, la Convention de Budapest, qui permet, en théorie, aux autorités suisses de requérir des informations d'un prestataire de services localisé à l'étranger et actif sur sol suisse (art.

18 de la Convention
sur la cybercriminalité) et donc d'exercer des prérogatives similaires à celles prévues par le *US CLOUD Act*.

2. US CLOUD Act – Partie 2

La deuxième partie du *US CLOUD Act* traite de la possibilité pour les États-Unis de conclure avec d'autres États un *executive agreement*, qui peut notamment régir les points suivants :

- Les États-Unis pourraient requérir directement (*i.e.*, hors entraide) des données auprès d'un Prestataire IT ayant son siège dans l'État contractant (même si ce Prestataire IT n'a pas de lien particulier avec les États-Unis).
- A l'inverse, l'État contractant pourrait requérir directement (*i.e.*, hors entraide) des données détenues par un Prestataire IT ayant son siège aux États-Unis, pour autant que ces informations ne concernent pas une *US Person* (personne résidente aux États-Unis ou de nationalité américaine).
- Le Prestataire IT requis de fournir les données disposerait de la possibilité de contester, devant un tribunal américain, la demande des autorités américaines, pour autant que la personne concernée ne soit pas une *US Person*. Dans un tel cas, le tribunal américain procédera à une pesée des intérêts, en prenant en compte notamment (i) les intérêts des États-Unis, et particulièrement ceux de l'autorité qui souhaite obtenir les informations, (ii) les relations entre la personne visée et les États-Unis, (iii) la probabilité d'une sanction (dans l'État du Prestataire IT requis) ainsi que sa sévérité, (iv) la probabilité d'accéder aux données par d'autres canaux (*e.g.*, l'entraide internationale) et (v) l'importance des données concernées pour l'enquête (section 2713 (h) (3) du *US CLOUD Act*).

A l'heure actuelle, le seul *executive agreement* en vigueur a été conclu entre les États-Unis et le Royaume-Uni le 3 octobre 2021. Depuis 2019, des négociations seraient en cours entre les États-Unis et l'Union européenne. Quand bien même les États-Unis souhaiteraient que ces négociations aboutissent à un *executive agreement*, il semblerait que l'Union européenne entend plutôt régler des problèmes d'application de sa législation sur les preuves électroniques.

II. Compatibilité du *US CLOUD Act* avec le droit suisse

La question de la « compatibilité » du *US CLOUD Act* avec la législation suisse concerne en premier lieu les Prestataires IT qui sont basés en Suisse et, potentiellement, soumis à une

obligation de divulgation d'informations en raison de l'application extraterritoriale du *US CLOUD Act*. Cela étant dit, les entreprises suisses qui confient des données (en particulier des données personnelles) à un Prestataire IT doivent également tenir compte de cette problématique, dans la mesure où ces entreprises suisses ont un rôle de *data controller* (responsable de traitement) qui assume une responsabilité règlementaire (art. 10a LPD et art. 9 nLPD) pour les activités de son *data processor* (sous-traitant, typiquement le Prestataire IT).

1. *Compatibilité avec le droit suisse de la protection des données ?*

Le Rapport reflète certains points de friction entre le *US CLOUD Act* et la LPD :

- Selon le principe de proportionnalité (art. 4 al. 2 LPD et art. 6 al. 2 nLPD), les droits de la personne concernée doivent être préservés au mieux et un rapport raisonnable entre les finalités du traitement et les moyens utilisés doit exister. Le Rapport indique que la transmission par le biais du *US CLOUD Act* ne constitue pas un moyen particulièrement respectueux des droits des personnes concernées.
- Ensuite, lors de la collecte de données, les finalités du traitement doivent être déterminées et reconnaissables pour la personne concernée (art. 4 al. 3 et 4 LPD et art. 6 al. 3 nLPD). Comme l'indique le Rapport, la divulgation par le Prestataire IT de données personnelles en réponse à une requête fondée sur le *US CLOUD Act* constitue une modification de la finalité du traitement qui doit être communiquée à la personne concernée. Or le *US CLOUD Act* prévoit que le Prestataire IT a, dans certains cas, l'interdiction de prévenir la personne concernée de la transmission de ses données.
- Le *US CLOUD Act* entre également en conflit avec les règles relatives à la communication transfrontalière de données (art. 6 LPD et art. 16 à 18 nLPD). En effet, les États-Unis n'offrent pas un niveau de protection des données adéquat au sens de l'art. 6 LPD, ce qui signifie que la transmission doit être basée sur l'un des motifs justificatifs figurant à l'art. 6 al. 2 LPD (respectivement à l'art. 17 nLPD). Or ce n'est que dans des cas exceptionnels que le motif justificatif de l'« intérêt public » (art. 6 al. 2 let. d LPD et art. 17 al. 1 let. c nLPD) pourra être invoqué.

2. *Compatibilité avec le droit suisse de l'entraide ?*

La communication directe d'informations à travers le canal prévu par le *US CLOUD Act* équivaut, dans les faits, à un contournement des mécanismes d'entraide internationale, qui prévoient une série de droits procéduraux en faveur de la personne concernée et une intervention d'une autorité suisse. Un mouvement similaire s'est déjà manifesté dans le domaine fiscal (avec le passage à l'échange automatique de renseignements) et dans le domaine

financier (avec l'adoption de la Circulaire FINMA 2017/6, Transmission directe, qui réserve toutefois à ses chiffres 30–31 et 42 le respect des droits des personnes concernées, notamment en matière de protection des données).

3. *Compatibilité avec l'art. 271 CP*

Même si ce point n'est (curieusement) pas mentionné dans le Rapport (hormis une brève référence, en page 47, à une « autorisation »), la communication depuis la Suisse de données personnelles à une autorité américaine pourrait également entraîner des conséquences pénales sous l'angle de l'art. 271 CP. En effet, cette disposition punit celui qui, sans y être autorisé, aura procédé sur le territoire suisse, pour un État étranger, à des actes qui relèvent des pouvoirs publics. En particulier, la personne qui remet des informations concernant des tiers, qui sont protégées par l'ordre public suisse, à une autorité étrangère en dehors de l'entraide administrative ou judiciaire, ou sans autorisation, pourrait encourir une responsabilité pénale sous l'angle de l'art. 271 CP (cf. notamment l'arrêt de la Cour des plaintes du Tribunal pénal fédéral CA.2019.6 du 5 décembre 2019, c. 1.1.1).

III. Est-ce que la Suisse devrait conclure un *executive agreement* ?

Comme mentionné plus haut, les États ont la possibilité de conclure un *executive agreement* avec les États-Unis pour régler plusieurs éléments d'application du *US CLOUD Act*.

Bien que cet accord bilatéral puisse amener certains éléments positifs (par exemple : définition plus précise de la notion de *serious crime*, possibilité pour le Prestataire IT de contester devant les tribunaux américains la demande de renseignements des autorités américaines si la demande ne concerne pas une *US Person*), l'on conçoit mal qu'un tel accord puisse pallier les incompatibilités du *US CLOUD Act* avec le droit suisse, qui ont été mises en exergue ci-dessus. L'Association suisse des banquiers (ASB) a publié une prise de position qui recense les exigences minimales que devraient contenir un *executive agreement* (notamment : exclure du champ d'application des injonctions à l'encontre de sociétés ayant leur siège en Suisse, limiter le cercle des personnes concernées aux *US Persons*, possibilité de se prévaloir du secret bancaire) afin d'être acceptable pour l'industrie financière. Il semble peu vraisemblable que ces exigences puissent être agréées par les États-Unis. Par ailleurs, la conclusion d'un *executive agreement* s'accompagnerait probablement d'une non-application de l'art. 271 CP aux communications couvertes par un tel *executive agreement*, alors même que cette disposition pénale offre aujourd'hui une certaine assurance aux clients des Prestataire IT basés en Suisse : en effet, les employés de ces derniers sont exposés à un risque pénal en cas de transmission d'informations aux États-Unis.

Finalement, la conclusion d'un *executive agreement* pourrait également avoir un impact négatif sur le maintien de la décision d'adéquation dont bénéficie le droit suisse de la protection des données (art. 45 RGPD), étant précisé que la Commission européenne est toujours en train d'examiner le maintien de cette déclaration suite à l'entrée en vigueur du RGPD. La conclusion d'un *executive agreement* (pour autant que celui-ci ne reflète pas des termes similaires à un potentiel accord entre les États-Unis et l'Union européenne) ne serait pas un élément favorable en vue du maintien de cette déclaration d'adéquation.

IV. Conclusion

Le *US CLOUD Act*, lu en parallèle avec les dispositions de la nouvelle LPD (qui érigent au rang d'infraction pénale le non-respect des règles suisses en matière de partage transfrontalier de données personnelles, art. 61 let. a nLPD) et avec la position stricte du Préposé fédéral à la protection des données et à la transparence dans le contexte de la transmission de données personnelles vers des États réputés « non-adéquats » (Guide pour l'examen de la licéité de la communication transfrontalière de données du 28 juin 2021), doit clairement être un point d'attention pour toute entreprise suisse qui envisage de confier le traitement (y compris le stockage) de données personnelles (en *clear text*) à un Prestataire IT. Tel sera typiquement le cas des prestataires de services en matière de *cloud computing*, tels que Microsoft, Amazon et Google. L'analyse du risque découlant du *US CLOUD Act* doit également intervenir si la partie cocontractante est l'entité suisse ou européenne (par exemple irlandaise dans le cas de Microsoft) du groupe. De même, l'analyse de risque doit également être déclenchée si un sous-traitant du prestataire de services présente un lien avec les États-Unis, pour autant naturellement que ce sous-traitant ait accès aux données en *clear text*.

Cela étant dit, le *US CLOUD Act* ne doit pas non plus entraîner le blocage complet de tout projet impliquant un prestataire soumis à cette législation. Il convient en effet de rappeler que les modalités d'accès à l'information prévue par la Partie 1 du *US CLOUD Act* sont limitées aux situations de *serious crimes*. Par ailleurs, le risque lié au *US CLOUD Act* peut être limité (sans être supprimé totalement) en travaillant sur les trois axes suivants :

- Préparation d'une analyse de risque documentée qui explique les raisons qui ont amené le responsable de traitement à initier un projet nonobstant les risques résiduels découlant du *US CLOUD Act*.
- Introduction de clauses spécifiques dans le rapport avec le Prestataire IT (par exemple une « *defend your data clause* » ; sur les éléments à prendre en considération dans le contrat avec le Prestataire IT, voir notamment swissprivacy.law/27).
- Information transparente des personnes concernées et, éventuellement, un consente-

ment (art. 6 al. 2 let. b LPD et art. 17 al. 1 let. a nLPD) de celles-ci.

L'on relèvera qu'une juridiction française (le Conseil d'État) a estimé, certes dans le cadre d'une ordonnance statuant en référé, que le risque d'une divulgation fondée sur le *US CLOUD Act* ne constituait pas, en tant que tel, un transfert de données personnelles vers un État « non adéquat » (sur ce point : voir notamment Marine Largant/Philipp Fischer, Health Data Hub, in : Jusletter 7 juin 2021). Ainsi, selon cette ordonnance, ce risque ne déclenche pas les exigences découlant de l'arrêt Schrems II (décision de la CJUE n° C-311/18) et, donc, des prises de position subséquentes des autorités (Recommandations du Comité Européen de la Protection des Données de juin 2021 ; en Suisse, le Guide pour l'examen de la licéité de la communication transfrontalière de données du Préposé fédéral à la protection des données et à la transparence du 28 juin 2021 est pertinent dans ce domaine).

En dernier lieu, l'on rappellera que le *US CLOUD Act* ne constitue pas l'unique prisme par lequel un projet d'externalisation de données doit être analysé. L'impératif de sécurité des données (à savoir la protection contre des intrusions de tiers qui ne sont pas acteurs gouvernementaux) et la nécessité de garantir la *business continuity* représentent des enjeux tout aussi importants, voire même plus cruciaux en termes de risques effectifs pour les données personnelles confiées à un tiers.

Proposition de citation : Philipp Fischer / Sébastien Pittet, *US CLOUD Act* – un aperçu, 8 novembre 2021 *in* www.swissprivacy.law/101