EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
*La voix de la profession d'avocat en Europe*

Rue Joseph II, 40/8 - B-1000 Bruxelles
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

# Évaluation du CCBE de la loi *CLOUD Act* des États-Unis

28/02/2019

*Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million d'avocats européens. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.*

Dans ce document, le CCBE présente son analyse de la loi américaine « Clarifying Lawful Overseas Use of Data Act » (*CLOUD Act*) et évalue dans quelle mesure ses dispositions sont conformes au droit européen.

## A. Résumé des dispositions du *CLOUD Act*

Le 22 mars 2018, le Congrès des États-Unis a adopté le *CLOUD Act* qui modifie le Code des États-Unis afin d'y insérer des dispositions nouvelles ou modifiées concernant l'accès du gouvernement des États-Unis aux données stockées hors des États-Unis et l'accès par des gouvernements étrangers à des données stockées aux États-Unis. La loi a été adoptée, sans véritable examen, dans le cadre de la loi de finances *Appropriations Act 2018*, une mesure « omnibus ».

Le plus important d'un point de vue européen est que le *CLOUD Act* modifie le chapitre 121 du titre 18 du Code des États-Unis en ajoutant au Code un nouveau § 2713 intitulé « conservation et divulgation obligatoires des communications et des enregistrements ».

L'ajout indique que la loi *Stored Communications Act* (« SCA ») existant s'applique également aux données stockées en *dehors* des États-Unis. Le SCA avait introduit les §§ 2703 et suivants au Code des États-Unis en 1986 dans le but d'imposer des obligations juridiques de confidentialité aux fournisseurs d'informations et de prescrire les circonstances dans lesquelles le gouvernement peut exiger la divulgation de communications électroniques stockées à distance[1]. La disposition la plus importante du SCA pour une meilleure compréhension du *CLOUD Act* est le § 2703 du Code des États-Unis. Cette disposition décrit en détail les règles en vertu desquelles une entité gouvernementale peut exiger qu'un prestataire fournisse des informations et les moyens d'y avoir accès. Il s'agit *soit de l'*obtention d'un mandat délivré conformément aux Règles fédérales de procédure pénale (sans notification à l'abonné ou au client)*, soit* d'une citation à comparaître devant un tribunal administratif ou un grand jury, soit d'une injonction (avec information la personne concernée), voir § 2703(b)(1)(A-B). Étant donné qu'il n'est habituellement pas souhaitable d'informer l'abonné ou le client, l'évaluation juridique des dispositions du *CLOUD Act* qui suit sera fondée sur l'hypothèse que la divulgation sera normalement demandée au moyen d'un mandat.

L'impulsion immédiate pour l'adoption du *CLOUD Act* a été l'affaire *Microsoft Warrant* (*United States v Microsoft, affaire 17-2 de la Cour suprême des États-Unis)* qui visait à déterminer si la récupération par le gouvernement des États-Unis de données stockées à l'étranger constituait une « recherche nationale » légale en vertu de la loi en question, étant donné qu'il était possible de récupérer ces

[1] cf. S. REP. 99-541, 5, 1986 U.S.C.C.C.A.N. 3555, 3559.

données en y ayant accès depuis un terminal informatique situé aux États-Unis. Le gouvernement des États-Unis a soutenu qu'il l'avait fait, mais Microsoft (qui a gagné devant la *Circuit Court of Appeals* des États-Unis) a fait valoir qu'il ne l'avait pas fait et a été soutenu devant la Cour suprême américaine par un certain nombre d'*amici curiae* (dont le CCBE) qui ont également soumis des mémoires[2]. Après la conclusion des plaidoiries et pendant que la Cour examinait sa décision, le *CLOUD Act* a été promulgué et le gouvernement des États-Unis a abandonné son appel, laissant l'interprétation correcte du SCA en suspens. Maintenant, le nouveau § 2713 du Code des États-Unis indique :

> « Un fournisseur de services de communications électroniques ou de services informatiques à distance [en particulier d'informatique en nuage] doit se conformer à l'obligation du présent chapitre [§§ 2703 et suivants] de préserver, sauvegarder ou divulguer le contenu d'un fil ou d'une communication électronique et tout enregistrement ou autre information concernant un client ou abonné en sa possession, sous sa garde ou son contrôle, que ces communications, enregistrements ou autres informations soient situés aux États-Unis ou à l'étranger. »

Le § 2703 du Code des États-Unis permet à toute entité gouvernementale américaine d'émettre un mandat afin d'exiger la divulgation prévue au § 2713 du Code des États-Unis. Dans le cas où un tel « fournisseur de services de communications électroniques ou de services informatiques à distance » basé aux États-Unis reçoit un mandat, le § 2703 prévoit une voie de recours par laquelle il peut demander que le mandat soit déclaré nul (« annulé ») ou modifié par un tribunal américain (« § 2703 (h) (2) requêtes pour annulation ou modification »).

Le fournisseur doit déposer la requête appropriée dans les 14 jours suivant la signification du mandat en démontrant ce qui suit :

> « (i) que le client ou l'abonné n'est pas un ressortissant des États-Unis et ne réside pas aux États-Unis; et
>
> (ii) que la divulgation requise créerait un risque important que le fournisseur viole les lois d'un gouvernement étranger admissible » (§ 2703 (h) (2) du Code des États-Unis) »

Par « gouvernement étranger admissible », on entend tout gouvernement étranger qui a conclu un accord exécutif avec les États-Unis, voir § 2703 (h) (1). La Cour saisie de la question peut approuver la requête du fournisseur, après avoir également entendu le gouvernement des États-Unis, s'il le juge nécessaire :

> « (i) la divulgation requise inciterait le fournisseur à enfreindre les lois d'un gouvernement étranger admissible ;
>
> (ii) compte tenu de l'ensemble des circonstances, les intérêts de la justice exigent que le processus judiciaire soit modifié ou annulé ; et
>
> (iii) le client ou l'abonné n'est pas un ressortissant des États-Unis et ne réside pas aux États-Unis. » (§ 2703 (h) (2) (B) du Code des États-Unis) »

L'aspect (ii) exige une « analyse de courtoisie » fondée sur huit autres critères que la Cour doit prendre en considération :

> « (A) les intérêts des États-Unis, y compris les intérêts d'enquête de l'entité gouvernementale qui cherche à obtenir la divulgation ;
>
> (B) l'intérêt du gouvernement étranger admissible à empêcher toute divulgation interdite ;
>
> (C) la probabilité, l'étendue et la nature des pénalités imposées au fournisseur ou à ses employés en raison d'exigences juridiques incompatibles imposées au fournisseur ;

[2] Mémoire du CCBE en tant qu'amicus curiae à l'appui de l'intimé dans l'affaire Microsoft Ireland

(D) la localisation et la nationalité de l'abonné ou du client dont les communications sont recherchées, si elles sont connues, ainsi que la nature et l'étendue aux États-Unis [...] ;

(E) la nature et l'étendue des liens et de la présence du fournisseur aux États-Unis ;

(F) l'importance, pour l'enquête, des renseignements devant être divulgués ;

(G) la probabilité d'un accès rapide et efficace à l'information devant être divulguée par des moyens qui entraîneraient des conséquences négatives moins graves ; et

(H) si la procédure judiciaire [à savoir le mandat] a été demandée au nom d'une autorité étrangère en vertu du § 3512, les intérêts de l'autorité étrangère qui présente la demande d'assistance. » (§ 2703 (h) (3) du Code des États-Unis) »

Les destinataires potentiels du § 2713 sont des sociétés Internet telles que Google, des réseaux sociaux tels que Facebook, Instagram et Twitter, ainsi que des fournisseurs de technologies dans le nuage, des registres de noms de domaine, des bureaux d'enregistrement et des « places de marché numériques » qui permettent aux consommateurs ou aux commerçants de conclure des transactions *peer-to-peer*[3].

Le § 2713 du Code des États-Unis, à première vue, ne s'applique qu'aux sociétés basées aux États-Unis. Toutefois, les mandats extraterritoriaux des États-Unis pourraient s'appliquer aux sociétés étrangères s'il existe un lien juridictionnel suffisant. Ainsi, le service de messagerie Telegram, bien que n'étant pas une personne américaine, pourrait faire l'objet d'une injonction puisqu'il dessert des clients états-uniens[4].

### B. Changements positifs découlant du *CLOUD Act*

Le CCBE considère comme une évolution positive le fait que l'accès gouvernemental aux données stockées en dehors des États-Unis repose désormais sur un cadre juridique établi qui définit également les procédures selon lesquelles les fournisseurs de services peuvent contester un mandat. Cela crée un plus grand degré de sécurité juridique pour les prestataires de services que sous l'ancien régime SCA, dans lequel les prestataires étaient tenus d'intenter une action en justice pour ne pas avoir à se conformer à un mandat (comme, par exemple, dans l'affaire du mandat Microsoft).

En outre, le CCBE reconnaît l'incitation (voir le § 2523 du Code des États-Unis tel que modifié) pour les gouvernements étrangers à conclure des accords exécutifs avec les États-Unis sur l'accès aux données concernant les ressortissants ou résidents permanents des États-Unis. En raison d'accords exécutifs en vertu du § 2523 du Code des États-Unis, les prestataires de services sont autorisés à répondre aux demandes d'information émanant de gouvernements étrangers, ce qui facilite les demandes d'information transfrontalières. Si, en principe, le CCBE se félicite de ces avancées vers la formalisation des processus transfrontaliers, celles-ci n'en demeurent pas moins réellement préoccupantes, notamment en raison de l'approche unilatérale adoptée par la législation.

### C. Préoccupations générales concernant le CLOUD Act

#### I. Procédure législative courte

Le *CLOUD Act* n'a fait l'objet d'aucune audience en comité, ni à la Chambre ni au Sénat. Le CCBE estime qu'une telle procédure législative tronquée est particulièrement surprenante, étant donné que la même question juridique a été fortement contestée dans l'*affaire Microsoft* devant la Cour suprême. La Cour suprême a eu à traiter de nombreux mémoires d'*amicus curiae* contenant des arguments

3 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

4 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom#_ftn1.

solides tant pour que contre la légitimité de l'injonction de divulgation en question[5]. Bien que la question de la nécessité d'une évaluation juridique de la requête et de la manière dont elle doit être évaluée ait été traitée par le *CLOUD Act*, la complexité factuelle de ces requêtes n'a pas changé. Le CCBE aurait donc souhaité que le *CLOUD Act* fasse l'objet d'un débat complet et approfondi.

II. Compétence extraterritoriale

Le *CLOUD Act* accorde aux organismes chargés de l'application de la loi une compétence illimitée sur toutes les données contrôlées par un fournisseur de services ayant des facteurs de connexion suffisants avec les États-Unis (voir ci-dessus).

Par conséquent, les procédures bien établies pour permettre l'accès aux données personnelles stockées en dehors de la juridiction d'un pays, telles que les traités d'entraide judiciaire, sont ignorées et les efforts pour les adapter aux nouveaux défis sont sapés. Le CCBE considère qu'il s'agit là d'une évolution indésirable et suggère qu'il serait plus approprié que les règles et procédures d'accès des forces de l'ordre aux données personnelles stockées dans des juridictions étrangères soient formulées par consensus et accord international.

Le Parlement européen a abordé la question dans sa résolution sur la cybercriminalité en exprimant ce qui suit

« inquiétude en ce qui concerne le champ d'action extraterritorial des services répressifs qui doivent accéder à des données dans le contexte d'enquêtes pénales, et souligne la nécessité de mettre en œuvre des règles strictes à cet égard »[6],

tout en demandant dans le même temps à la Commission européenne de s'opposer à l'élargissement de

> « l'appropriation de la compétence extraterritoriale par des pays tiers »

De manière beaucoup plus explicite, le Parlement européen a fait part de sa préoccupation le 5 juillet 2018, notant que le *CLOUD Act*

> « étend les compétences des services répressifs américains et étrangers en leur permettant de cibler et d'accéder aux données des personnes au-delà des frontières internationales sans recourir aux instruments d'entraide judiciaire (MLAT), qui eux prévoient des garanties appropriées et respectent les compétences judiciaires des pays sur le territoire desquels l'information est stockée ».[7]

et a pris en considération le fait

> « qu'une solution plus équilibrée aurait été de renforcer le système international existant de traités d'entraide judiciaire en vue d'encourager la coopération internationale et judiciaire ; [en particulier parce que], comme le prévoit l'article 48 du règlement général sur la protection des données, l'entraide judiciaire et d'autres accords internationaux constituent le mécanisme privilégié pour permettre l'accès aux données personnelles à l'étranger ».[8]

---

5 *Ibid*.

6 Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI)), art. 63 et 80, disponibles à l'adresse http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//FR

7 Résolution du Parlement européen du 5 juillet 2018 sur le caractère adéquat de la protection offerte par le bouclier de protection de la vie privée UE/États-Unis, considérant 27, disponible à l'adresse http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//FR

8 Résolution du Parlement européen du 5 juillet 2018 sur le caractère adéquat de la protection offerte par le bouclier de protection de la vie privée UE/États-Unis, considérant 28, disponible à l'adresse http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//FR

De plus, le *CLOUD Act* crée un précédent dangereux pour d'autres pays. Il crée un précédent pour tout pays qui est déterminé à exiger la récupération des données stockées n'importe où dans le monde en se basant uniquement sur l'autorité judiciaire de ce pays. Le CCBE exprime ses vives réserves à l'égard de ces mesures, qui ont pour effet l'extension unilatérale de la juridiction étendue.

III. Lois conflictuelles

Le *CLOUD Act* est contraire aux droits humains élémentaires étant donné qu'il ne prévoit pas les normes minimales fixées par les cours européennes pour restreindre la surveillance électronique par le gouvernement. Tant la Cour européenne des droits de l'homme que la Cour de justice de l'Union européenne ont indiqué une forte préférence pour un contrôle juridictionnel préalable et l'exigence d'une base factuelle suffisante pour toute surveillance d'un individu.

En outre, la divulgation de données à caractère personnel stockées dans l'Union européenne à une agence gouvernementale américaine à partir d'un mandat en vertu du *CLOUD Act* constitue une violation du Règlement général sur la protection des données (RGPD). Selon les dispositions du RGPD, un mandat des États-Unis ne constitue pas une base juridique pour un tel transfert en dehors de l'Union européenne.[9]

*Droits fondamentaux*

L'article 8 de la Convention européenne des droits de l'homme et les articles 7 et 8 de la Charte européenne des droits fondamentaux reconnaissent un droit fondamental à la vie privée. Selon la jurisprudence de la Cour européenne des droits de l'homme et de la Cour européenne de justice, toute ingérence dans le droit à la vie privée doit être conforme à la loi, avoir un but légitime et se limiter à ce qui est nécessaire dans une société démocratique[10]. En ce qui concerne le droit à la protection des données, les deux cours appliquent une norme de « stricte nécessité ».[11] Tant la Cour européenne des droits de l'homme (appliquant la Convention européenne) que la Cour européenne de justice (appliquant la Charte européenne) ont établi de nombreuses garanties pour le contrôle gouvernemental des communications électroniques.[12]

a) Absence de notification et de voies de recours

Le *CLOUD Act* ne dispose pas d'un système complet de protection de la vie privée par des normes procédurales et organisationnelles. Aucune notification n'est donnée à quelque niveau que ce soit. Ni l'État où les données sont stockées ni l'État dont la personne concernée est citoyenne ne sont informés. Mais surtout, selon la Cour européenne des droits de l'homme, la notification et un recours effectif devraient être fournis à la personne concernée étant donné que la notification est liée à l'efficacité des recours. Dans l'affaire *Szabó*, la Cour européenne des droits de l'homme a estimé qu'une notification doit être communiquée dès que les mesures de surveillance prennent fin et que la notification ne compromet plus les enquêtes.

En ce qui concerne les voies de recours, le *CLOUD Act* porte également atteinte à l'article 19 de l'Accord entre les États-Unis et l'Union européenne sur la protection des renseignements personnels en matière de prévention, d'investigation, de détection et de poursuite des infractions pénales (DPPA). L'article

[9] Voir Mémoire du CCBE en tant qu'amicus curiae à l'appui de l'intimé dans l'affaire Microsoft Ireland.

[10] Par exemple, Cour européenne des droits de l'homme, Liberty c. Royaume-Uni, App. No 58243/00, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2258243/00%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-87208%22]}

[11] Cour européenne des droits de l'homme, Szabó, requête 37138/14, p. 33 ; Cour européenne de justice, Digital Rights Ir. Ltd. c. Ministre de la Marine et du Nord canadien.

[12] Cour européenne des droits de l'homme, Zakharov c. Russie, requête 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}

19 du DPPA impose aux parties l'obligation de prévoir, dans leur droit interne, des droits de recours judiciaires spécifiques pour leurs citoyens respectifs.

b) Portée et durée imprécises des mesures de surveillance

Le *CLOUD Act* ne prévoit pas de limites adéquates en ce qui concerne la portée et la durée des mesures de surveillance.

Rien n'indique dans quelles circonstances les autorités publiques sont habilitées à recourir aux mesures de surveillance décrites dans le *CLOUD Act*. La Cour européenne des droits de l'homme exige une définition claire à la fois de la « nature des infractions qui peuvent donner lieu » à une injonction et d'une « définition des catégories de personnes susceptibles » d'être surveillées[13]. À titre de garantie minimale à cet égard, le *CLOUD Act* devrait préciser la nature des infractions auxquelles elle s'applique, soit en précisant la nature de ces infractions, soit en faisant au moins référence aux niveaux minimaux de sanction autorisés.

La Cour européenne des droits de l'homme a clarifié que cette double exigence ne signifie pas qu'un individu doive être en mesure de prévoir quand les autorités sont susceptibles d'intercepter ses communications afin d'adapter son comportement en conséquence. La « prévisibilité » signifie davantage l'existence de conditions préalables claires et détaillées afin de minimiser le risque de décisions arbitraires. Dans l'affaire *Weber c. Allemagne* (requête 54934/00), la Cour européenne des droits de l'homme a estimé qu'une loi était raisonnablement prévisible en se fondant sur le fait que la loi précisait les infractions exactes pour lesquelles la surveillance pouvait être ordonnée et exigeait que la cible ait passé des appels téléphoniques internationaux en utilisant des technologies spécifiques ou en prononçant des mots clés spécifiques (considérant 97 de l'arrêt, où il était précisé que les personnes concernées devaient avoir participé à une conversation téléphonique internationale par l'intermédiaire de relais satellites ou hertziens (ou encore par l'intermédiaire de lignes téléphoniques fixes dans le cas d'une surveillance visant à la prévention d'une attaque armée contre l'Allemagne, d'après l'article 3 § 1, point 1)..

Les restrictions appropriées quant à la durée comprennent une indication claire de la période après laquelle un mandat d'interception expire, des conditions dans lesquelles il peut être renouvelé et des circonstances dans lesquelles il doit être annulé. Aucune disposition du *CLOUD Act* ne prévoit de tels délais.

c) Mesures de protection supplémentaires

En vertu de la Convention européenne, la légalité et la nécessité d'un régime de surveillance sont évaluées en fonction de l'accessibilité du droit interne, des procédures à suivre pour stocker, accéder, examiner, utiliser, communiquer et détruire les données interceptées, des procédures d'autorisation et des modalités de contrôle de l'application des mesures de surveillance secrète[14].

Il est fort probable que les mandats délivrés en vertu du *CLOUD Act* ne répondront pas à la norme des cours européennes en matière de conditions de surveillance accessibles (c'est-à-dire accessibles au public). Par exemple, dans l'affaire *Liberty c. Royaume-Uni*, des rapports annuels dans lesquels le ministre de l'Intérieur britannique affirmait simplement, sans plus de détails, que des « mesures » garantissaient un accès restreint aux éléments recueillis par le biais de la surveillance, ont été estimés

[13] Cour européenne des droits de l'homme, Zakharov c. Russie, requête 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}

[14] Cour européenne des droits de l'homme, Zakharov c. Russie, requête 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}, p. 60.

n'avoir « aucune incidence sur la clarté et l'accessibilité des « mesures » en question puisqu'ils n'étaient pas habilités à en révéler le »[15].

Les données obtenues par mesure de surveillance ne doivent pas non plus être stockées sans limite. En principe, les données doivent être détruites immédiatement si elles ne sont plus pertinentes au regard de la finalité pour laquelle elles ont été obtenues[16]. Même si les données stockées sont pertinentes, leur conservation sur une plus longue période doit être justifiée par des critères objectifs[17]. Par exemple, aucune donnée ne peut être conservée sur des « personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves ».[18]

*RGPD*

Les mandats émis en vertu du *CLOUD Act* sont également en conflit avec le RGPD de l'UE. Un mandat à lui seul ne fournit généralement pas une base juridique pour le traitement des données dans le cadre du RGPD.

Le consentement ne peut pas justifier le traitement des données en vertu du *CLOUD Act* étant donné que la personne concernée n'est pas informée de l'émission du mandat. Toutefois, pour qu'un consentement soit valide, il faut que la personne soit suffisamment informée et qu'elle ait la possibilité de le retirer. Ces exigences ne sont pas respectées dans un environnement d'application de la loi.

L'article 6 (1)(c) du RGPD ne justifie pas non plus un tel traitement. Bien que l'article 6 (1)(c) reconnaît la nécessité « du respect d'une obligation légale à laquelle le responsable du traitement est soumis », cette obligation juridique doit découler du droit de l'UE. Par conséquent, une obligation en vertu du *CLOUD Act* ne constitue pas une obligation juridique au sens de l'article 6 (1)(c) du RGPD.

L'article 48 du RGPD prévoit ce qui suit :

> « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre.».

En vertu de cette disposition, seuls les traités d'entraide judiciaire ou des accords internationaux comparables fournissent une base admissible pour le transfert extraterritorial de données à caractère personnel. Par conséquent, le *CLOUD Act* ne constitue pas une base juridique pour le transfert de données vers les États-Unis en vertu de l'article 48 du RGPD. Un mandat des États-Unis ne répond donc pas aux exigences de l'article 48 pour le transfert de données de l'Europe vers les États-Unis.

Un transfert de données résultant d'un mandat *CLOUD Act* n'est pas non plus admis par l'article 49 du RGPD étant donné que cette exemption est restreinte et doit être interprétée strictement. Il est fort probable qu'un mandat délivré en vertu du *CLOUD Act* ne respectera pas les restrictions prévues à l'article 49 (1) du RGPD puisque le destinataire du mandat (c'est-à-dire le fournisseur de services) ne

---

[15] Cour européenne des droits de l'homme, Liberty c. Royaume-Uni, requête 58243/00, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2258243/00%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-87208%22]}.

[16] Cour européenne des droits de l'homme, Zakharov c. Russie, requête 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}, p. 64.

[17] Cour de justice de l'Union européenne, Digital Rights Ir. Ltd. c. Ministre de la Marine et du Nord canadien, Ministre de la Marine et du Nord canadien. Rés. à la p. 63.

[18] Cour de justice de l'Union européenne, Digital Rights Ir. Ltd. c. Ministre de la Marine et du Nord canadien.

sera pas en mesure d'évaluer les circonstances du transfert de données étant donné que le gouvernement pourrait ne pas être disposé à divulguer des renseignements sur la surveillance. En outre, la dérogation de l'article 49 (1)(d) ne s'applique pas étant donné que l'intérêt public ne peut pas être fondé sur une décision unilatérale d'un pays tiers[19].

En tant que destinataires d'un mandat en vertu du *CLOUD Act*, les entreprises technologiques se trouveront entre deux lois contradictoires sur les données. Étant donné que le RGPD limite strictement les circonstances dans lesquelles les données peuvent être légalement transférées à des pays tiers et prévoit de lourdes amendes en cas de violation (allant jusqu'à 4 % du chiffre d'affaires d'une entreprise), les entreprises sont prises entre le non-respect d'un mandat des États-Unis (pour violation d'une ordonnance du *CLOUD Act*) et le risque de sanctions monétaires voire pénales importantes (pour violation des dispositions du RGPD). Les lois nationales qui complètent le RGPD prévoient des peines de prison allant jusqu'à trois ans pour les violations du RGPD (article 42 (1) de la nouvelle loi fédérale allemande sur la protection des données).

IV. Voies de recours limitées pour le fournisseur de services concerné

Le CCBE salut le fait que le *CLOUD Act* garantisse que la surveillance ne soit pas ordonnée « au hasard, de manière irrégulière ou sans considération appropriée » en soumettant toute procédure autorisant la surveillance à un contrôle juridictionnel préalable.

Bien qu'il soit positif, comparativement à la situation antérieure au *CLOUD Act,* qu'il existe maintenant un processus bien établi pour contester un mandat avant son exécution, le recours possible est de portée limitée.

Les fournisseurs qui se trouvent dans un dilemme entre les obligations juridiques de l'UE et l'obligation de se conformer au mandat SCA/*CLOUD Act* se retrouvent une fois de plus à refuser de se conformer et à contester une ordonnance pour outrage étant donné qu'ils ne sont pas en mesure de déposer la requête pour modifier ou annuler le mandat. Cela s'explique par le fait que l'UE, tel qu'expliqué ci-dessus, ne relève pas du terme « gouvernement qualifié » parce qu'il s'agit d'une organisation supranationale. Le fournisseur n'est alors pas en mesure de déclarer un « risque important qu'il enfreindrait les lois du gouvernement étranger admissible » en suivant le mandat. Un tel raisonnement de risque important est cependant une condition préalable essentielle à la motion, comme l'indique le mot « et » au § 2713 du Code des États-Unis.

Même si, toutefois, l'expression « gouvernement qualifié » devait être interprétée au sens large de manière à s'appliquer aux organisations supranationales telles que l'UE, l'UE est probablement empêchée de conclure un accord exécutif en vertu du § 2523 du Code des États-Unis en raison de l'article 48 du RGPD (voir ci-dessus). Il en va de même pour les États membres de l'UE eux-mêmes étant donné qu'ils sont également liés par l'article 48 du RGPD. Au lieu de cela, il serait nécessaire que les États-Unis concluent un accord international tel qu'un traité d'entraide judiciaire avec l'UE ou avec tous les États membres de l'UE, ce que les États-Unis ne semblent pas disposés à entreprendre jusqu'ici.

En conséquence, le contrôle juridictionnel préalable à l'exécution est en fait inexistant pour les abonnés et les clients qui sont citoyens d'un État membre de l'UE.

Un contrôle juridictionnel préalable à l'exécution du mandat devrait être effectué indépendamment du fait que l'État dans lequel les informations requises sont stockées soit ou non un « gouvernement qualifié ». L'exigence (ii) relative au dépôt d'une requête s'y rapportant devrait donc être modifiée en : « (ii) que la divulgation requise créerait un risque important que le fournisseur viole les lois de l'État étranger où se trouve l'information demandée. »

[19] Voir également les lignes directrices 2/2018 du Conseil européen de la protection des données sur les dérogations à l'article 49 du règlement 2016/679, pages 10-11.

V. Faiblesse du contrôle (juridictionnel)

Comme expliqué précédemment, l'UE violerait ses propres lois, à savoir l'article 48 du RGPD, en concluant un accord exécutif en vertu du § 2523 du Code des États-Unis. Même si l'UE concluait un tel accord pour que ses intérêts soient reconnus dans le cadre du contrôle juridictionnel préalable à la suite d'une motion, les critères de courtoisie présentent toutefois des lacunes.

Premièrement, le « gouvernement étranger qualifié » (autre que le gouvernement américain) n'est pas entendu avant l'analyse de courtoisie. Il est donc probable que le tribunal compétent accordera plus de poids aux intérêts des États-Unis qu'aux intérêts du « gouvernement étranger qualifié » contre la divulgation.

Deuxièmement, étant donné que la nature et la gravité des infractions en question ne sont pas des conditions préalables à la délivrance du mandat, elles devraient au moins constituer un critère à prendre en considération dans l'analyse de courtoisie.

Troisièmement, le critère (F) relatif à l'importance de l'information pour l'enquête est interprété de façon trop large. Au lieu de cela, le § 2713 devrait indiquer qu'une divulgation n'est autorisée que dans le cas où l'enquête serait disproportionnellement plus difficile ou n'offrirait aucune perspective de succès.

Enfin, un contrôle juridictionnel préalable général serait souhaitable. En ce qui concerne l'analyse de courtoisie, le *CLOUD Act* devrait être modifié et passer de « (i) la divulgation requise inciterait le fournisseur à enfreindre les lois du gouvernement qualifié ; (...) » à « (i) la divulgation requise inciterait le fournisseur à enfreindre les lois de l'État où se trouve l'information demandée ». De même, les spécifications (A) à (H) avec cette référence devraient être modifiées.

VI. Absence de contrôle postérieur à l'autorisation

Le *CLOUD Act* ne prévoit aucun contrôle postérieur à l'autorisation. Pourtant, de telles dispositions de contrôle constituent une garantie vitale. Dans l'affaire *Schrems c. Data Protection Commissioner, la* Cour de justice de l'Union européenne a jugé qu'une autorité de contrôle nationale doit « examiner, en toute indépendance, toute demande relative à la protection des droits et libertés d'une personne à l'égard du traitement de données à caractère personnel la concernant ». Ce contrôle postérieur à l'autorisation pourrait prendre la forme d'une obligation de soumettre un rapport annuel sur les mesures ordonnées en vertu de la loi SCA/*CLOUD* à un comité de la Chambre des représentants. Le rapport pourrait être tenu d'indiquer le nombre de procédures engagées et les infractions pénales sous-jacentes auxquelles ces procédures se rapportent. Afin de garantir la transparence, le rapport devrait être obligatoirement publié.

## D. Absence de protection du secret professionnel et du *legal professional privilege*

I. Secret professionnel/*legal professional privilege* en général

Le CCBE est particulièrement préoccupé par le fait que le *CLOUD Act* ne tient pas compte de l'aspect particulièrement délicat des communications confidentielles entre les avocats et leurs clients. Toutes les associations professionnelles d'avocats de tous les États membres de l'UE considèrent que le secret professionnel est intrinsèque à la profession d'avocat. Il est évoqué dans tous les codes de déontologie nationaux, à l'instar de celui du CCBE[20]. La confidentialité fait partie de la déontologie de la profession d'avocat.[21]

[20] Conclusions de l'avocat général Poiares Maduro dans l'affaire C-305/05 devant la Cour de justice européenne, présentées le 14 décembre 2006, considérant 37.

[21] Conclusions de l'avocat général Poiares Maduro dans l'affaire C-305/05 devant la Cour de justice européenne, présentées le 14 décembre 2006, considérant 37.

Bien que les États européens adoptent des approches différentes en matière de protection du secret professionnel et du *legal professional privilege*, le principe d'une telle protection est généralement reconnu. Dans tous les États membres de l'UE (et dans les États membres du Conseil de l'Europe), elle a le rang de principe fondamental et le statut de règle d'ordre public[22].

L'article 41 de la Charte des droits fondamentaux de l'Union européenne énonce expressément la protection du secret professionnel, qui consacre

> « le droit d'accès de toute personne au dossier qui la concerne, dans le respect des intérêts légitimes de la confidentialité et du secret professionnel et des affaires ».

La reconnaissance du secret professionnel/*legal professional privilege* devant les tribunaux européens a une longue histoire, dans des juridictions individuelles antérieures à la fois à l'UE et au Conseil de l'Europe. Par sa jurisprudence, la Cour européenne de justice a confirmé le principe de la confidentialité des communications écrites entre un avocat et son client[23] et a reconnu la nature spécifique de la profession d'avocat[24].

La Cour européenne des droits de l'homme exige de tous les signataires de la Convention européenne de garantir le caractère sacré du secret professionnel ou du *legal professional privilege* sur leur territoire. Dans *Michaud c. France*, la Cour a souligné que l'échange entre les avocats et leurs clients bénéficiait d'une protection renforcée. La jurisprudence de la Cour européenne des droits de l'homme révèle deux principes différents qui sont à l'origine de la protection du secret professionnel et du *legal professional privilege*. Dans son arrêt *Niemietz c. Allemagne*, la Cour a jugé que, lorsqu'un avocat est impliqué, une atteinte au secret professionnel « peut se répercuter sur la bonne administration de la justice et, partant, sur les droits garantis par l'article 6 [le droit à un procès équitable] »[25]. Sans la certitude du secret, il n'y a pas de confiance dans la relation entre le client et l'avocat. En effet, aucun fondement ne pourrait conduire à la « manifestation de la vérité et de la justice »[26]. De même, l'avocat général Léger a déclaré dans ses conclusions dans l'affaire *Wouters e.a.* que « les avocats occupent une situation centrale dans l'administration de la justice, comme intermédiaires entre les justiciables et les tribunaux ».[27] Le secret professionnel est donc le corollaire essentiel du droit de défense du client.[28] Le deuxième aspect du secret professionnel/*legal professional privilege* est que le principe protège les justiciables des divulgations susceptibles de nuire à leur réputation. En ce qui concerne cet objectif de protection, la Cour européenne des droits de l'homme a jugé, dans son arrêt *Foxley c. Royaume-Uni,* que le droit à la vie privée en vertu de l'article 8 de la Charte européenne des droits de l'homme est une autre composante essentielle de ce principe[29].

En résumé, la protection du secret professionnel découle désormais de l'article 8, paragraphe 1 (protection de la correspondance) en lien avec l'article 6, paragraphes 1 et 3, point c), de la Charte européenne des droits de l'homme ainsi que de l'article 7 de la Charte des droits fondamentaux de l'Union européenne (respect des communications) en lien avec l'article 47, paragraphe 1, deuxième

---

22 Voir, à cet effet, le considérant 182 des conclusions de l'avocat général Léger dans l'affaire C-309/99, Wouters e.a., Cour de justice européenne.

23 Cour de justice de l'Union européenne, affaire 155/79, AM & S[1982], Recueil 1982, p. 1575.

24 Cour de justice de l'Union européenne, affaire C-309/99, Wouters et autres, Recueil 2002, p. 1-1577.

25 Cour européenne des droits de l'homme, arrêt du 16 décembre 1992, Niemietz c. Allemagne, § 37.

26 Conclusions de l'avocat général Poiares Maduro dans l'affaire C-305/05 devant la Cour de justice européenne, présentées le 14 décembre 2006, considérant 41.

27 Conclusions de l'avocat général Léger dans l'affaire C-309/99, Wouters et autres, considérant 174.

28 Cour de justice de l'Union européenne, affaire 155/79, AM & S contre Commission, Recueil 1982, p. 1575, points 10 et 23.

29 Cour européenne des droits de l'homme, arrêt du 10 septembre 2000, *Foxley c. Royaume-Uni*, § 44.

phrase du paragraphe 2 et l'article 48, paragraphe 2 (droit à être conseillé, représenté et défendu, respect des droits de la défense) de cette Charte.[30]

II. Absence de garanties procédurales

Le *CLOUD Act* menace de compromettre l'inviolabilité du conseil juridique sans offrir aux avocats ou à leurs clients aucune garantie procédurale pour protéger le secret professionnel accordé par le droit de l'UE.

Le droit de l'avocat européen à la protection du secret professionnel/*legal professional privilege* en ce qui concerne la saisie de matériel pouvant relever du secret et détenu sur des serveurs de données dans toute l'Europe n'est pas abordé dans le *CLOUD Act* et lei SCA respectivement. Toutefois, la Cour européenne des droits de l'homme a jugé qu'une saisie large et indifférenciée de la correspondance électronique violait le principe du du secret professionnel/*legal professional privilege*[31].

De même, l'avocate générale Kokott a déclaré ce qui suit dans l'affaire *Akzo et Akcros contre Commission* :

> « Si l'avocat, dans le cadre d'une procédure judiciaire ou de sa préparation, était obligé de coopérer avec les pouvoirs publics en leur transmettant des informations obtenues lors des consultations juridiques ayant eu lieu dans le cadre d'une telle procédure, celui-ci ne serait pas en mesure d'assurer sa mission de conseil, de défense et de représentation de son client de manière adéquate, et ce dernier serait par conséquent privé des droits qui lui sont conférés par l'article 6 de la CEDH, ainsi que par les articles 47 et 48 de la charte des droits fondamentaux (40). »[32]

Cela s'applique d'autant plus lorsque les avocats n'ont même pas connaissance de la saisie de matériel relevant du secret professionnel étant donné que la procédure de divulgation à la suite d'un mandat n'implique aucun préavis. Tant que le *CLOUD Act* ne prévoit pas l'irrecevabilité des preuves obtenues à partir de matériel relevant du secret professionnel, le *CLOUD Act* menace de priver les citoyens européens de leurs droits à la vie privée, à la représentation et à un procès équitable.

L'article 6 de la CEDH sur le droit à un procès équitable est absolu (contrairement à l'article 8 sur le droit à la vie privée, qui est spécifique) et pour cette raison, le CCBE suggère que l'existence du secret professionnel ou du *legal professional privilege* dans les données recherchées devrait être un obstacle absolu à la récupération de telles données. À cet égard, il convient de noter que du contenu relevant du secret professionnel et du *legal professional privilege* peut, dans certaines circonstances, se trouver dans les données relatives aux communications ainsi que dans les données relatives au contenu. Le secret professionnel et le *legal professional privilege* des avocats devraient au moins être mentionnés comme un facteur à prendre en compte dans « l'ensemble des circonstances » dans le cadre de l'analyse de courtoisie. Si cela n'est pas fait, le secret professionnel et le *legal professional privilege* ne seront probablement pas du tout pris en compte. Bien que les États-Unis reconnaissent l'« *attorney-client privilege* » comme règle de preuve absolue dont l'effet est que les défendeur au pénal ne sont pas obligés de produire au procureur des « rapports, mémorandums ou autres documents établis par le défendeur, ou son avocat ou agent, pendant l'enquête ou la défense » (règle fédéral de procédure pénale 16(b)(2)), l'application de ce principe est difficile pendant toute la procédure non contradictoire de collecte de preuve.

---

[30] Conclusions de l'avocat général Kokott dans l'affaire C-5550/07, rendue le 29 avril 2010, Akzo Nobel Chemicals et Akcros Chemicals contre Commission, considérant 47.

[31] Cour européenne des Droits de l'Homme, Vinci Construction et GTM Génie Civil et Services c. France, Requête. Nos 63629/10 et 60567/10, 2 avril 2015.

[32] Conclusions de l'avocat général Kokott dans l'affaire C-5550/07, rendues le 29 avril 2010, Akzo Nobel Chemicals et Akcros Chemicals contre Commission, considérant 49 avec renvoi complémentaire.

Il est d'autant plus important d'ajouter le secret professionnel et le *legal professional privilege* comme facteur de pondération à une analyse (générale) de courtoisie qu'il n'y a pas de contrôle juridictionnel après la saisie.

En outre, les obligations de secret professionnel dans certains pays européens peuvent avoir une portée plus large qu'aux États-Unis : en vertu du Code judiciaire belge, par exemple, la communication entre l'avocat et son client ne peut pas être utilisée comme preuve, et tout litige concernant le secret professionnel de l'avocat doit être résolu par le responsable du barreau belge[33]. Toute procédure de divulgation reposant sur un mandat *CLOUD Act* serait donc contraire au droit belge.

### E. Incidence sur le bouclier de la protection de la vie privée

En théorie, le *CLOUD Act* n'affecte pas le bouclier de protection des données étant donné que ce dernier s'applique au transfert transatlantique de données entre entités privées à des fins commerciales, tandis que le *CLOUD Act* s'applique au transfert transatlantique de données d'une entité privée à un organisme gouvernemental à des fins répressives et judiciaires. Dans la pratique, toutefois, le *CLOUD Act* ne fait rien pour prévenir le risque qu'après un transfert transatlantique à des fins commerciales des données à caractère personnel fassent l'objet d'une obligation de divulgation à des fins de poursuites. Les doutes quant au degré de protection que le bouclier de protection des données assure effectivement, qui ont été soulevés en particulier dans le cadre de l'affaire Microsoft, subsistent donc.

Il serait toutefois peu probable que la Commission modifie, en raison du *CLOUD Act*, son évaluation du caractère adéquat du bouclier de protection des données. Avant l'adoption du *CLOUD Act*, le gouvernement des États-Unis avait la possibilité d'accéder aux données personnelles d'un citoyen de l'UE, transférées aux États-Unis conformément au bouclier de protection des données et ensuite stockées aux États-Unis, sur le principe du SCA. Bien que le SCA n'ait prévu aucune voie de recours, la Commission est parvenue à la conclusion que les États-Unis garantissent un niveau adéquat de protection des données. Une évaluation beaucoup plus réaliste du niveau de protection des données aurait été de juger les prestataires de services états-uniens en ligne comme étant peu sûrs et non conformes aux dispositions du RGPD étant donné qu'il existe un risque de traitement sans restriction par les autorités des États-Unis après un mandat SCA. Comme ce risque persiste, les conclusions de la Commission quant au caractère adéquat du bouclier de protection des données demeurent à cet égard, discutables et doivent encore être remises en question.

### F. Recommandations

Afin d'éliminer le conflit entre le *CLOUD Act* et le droit européen, de créer des garanties et des voies de recours suffisantes contre les mesures de surveillance des États-Unis et de garantir la protection du secret professionnel et du *legal professional privilege*, le CCBE recommande que l'UE prenne les mesures suivantes :

1. négocier avec les États-Unis un traité d'entraide judiciaire faisant explicitement référence au *CLOUD Act*, prévoyant des exigences précises pour le transfert des données et ne portant pas atteinte au niveau de protection assuré par les libertés fondamentales ;
2. veiller à ce que, conformément à ce traité d'entraide judiciaire, dans chaque affaire, à la suite d'une demande de données en vertu du *CLOUD Act*, les données ne soient

[33] https://uk.practicallaw.thomsonreuters.com/2-103-2508?transitionType=Default&contextData=(sc.Default&firstPage=true&bhcp=1

transférées aux États-Unis qu'après notification à une autorité européenne compétente et indépendante ;

3. veiller à ce que le prestataire de services concerné qui héberge les données demandées soit informé par l'autorité européenne compétente des voies de recours existant aux États-Unis ;
4. veiller à ce que, conformément à ce traité d'entraide judiciaire, le secret professionnel et le *legal professional privilege* constituent un motif absolu d'objection au transfert de données aux États-Unis en vertu du *CLOUD Act*.