Qu'est-ce que le CLOUD Act ?

Le CLOUD Act (ou Clarifying Lawful Overseas Use of Data Act) a modifié l'ECPA (ou Electronic Communications Privacy Act – loi sur la confidentialité des communications électroniques), qui est la loi américaine régissant la manière dont les organismes chargés de l'application de la loi peuvent obtenir des informations détenues par certaines entreprises technologiques, y compris les fournisseurs de *cloud* (informatique en nuage).[1] Le CLOUD Act a été promulgué le 23 mars 2018.[2]

Le CLOUD Act contient deux sections. La première partie clarifie que les demandes d'accès émises en vertu de l'ECPA peuvent atteindre des données, quel que soit l'endroit où elles sont stockées.[3] La seconde partie crée un nouveau cadre pour les accords intergouvernementaux afin de régir les demandes transfrontalières d'application de la loi.[4]

Quand les données peuvent-elles être demandées aux entreprises technologiques en vertu du CLOUD Act ?

Les forces de l'ordre utilisent un mandat pour obtenir le contenu numérique d'un utilisateur. Un mandat ne peut être délivré que dans le cadre d'une enquête criminelle, et uniquement lorsqu'un juge estime qu'une série de garanties constitutionnelles et légales sont respectées.[5]

Le contenu numérique peut être demandé auprès des fournisseurs numériques :

- Uniquement dans le cadre d'enquêtes criminelles
- Uniquement après l'obtention d'un mandat approuvé par un tribunal indépendant
- Hors du cadre d'enquêtes de sécurité nationale

Le CLOUD Act n'autorise pas les demandes groupées.

- Le contenu numérique ne peut être demandé aux fournisseurs de technologies numériques qu'avec un mandat remis par un tribunal. Un mandat ne peut porter que sur des données identifiées avec précision dans le mandat lui-même, qui doit être approuvé par un tribunal indépendant.

LES DEMANDES D'ACCES DOIVENT RÉPONDRE AUX EXIGENCES LÉGALES

Toutes les conditions suivantes doivent être remplies lorsqu'un contenu numérique est demandé en vertu du CLOUD Act :

- L'organisme d'application de la loi doit enquêter sur un crime.
- L'organisme d'application de la loi doit demander un mandat à un tribunal.
- L'agent chargé de l'application de la loi doit prêter serment sur les faits présentés dans la demande de mandat.
- La demande de mandat doit décrire - avec précision - les informations recherchées.
- Un tribunal indépendant doit trouver que la demande de mandat établit un motif raisonnable que les informations recherchées contiennent des preuves d'un crime spécifique.

Les données d'entreprise font l'objet de mesures de protection supplémentaires :

- Lorsque le contenu appartient à une entreprise plutôt qu'à un individu, le département américain de la justice s'est engagé à "rechercher les données directement auprès de l'entreprise, plutôt qu'auprès de son fournisseur de services cloud, si cela ne compromet pas l'enquête."[6]
- Cet engagement reconnaît que dans de nombreux cas, l'entreprise cliente - et non le fournisseur de cloud - sera l'entité appropriée pour répondre à une procédure judiciaire.

Quelles sont les conditions requises pour émettre une demande d'accès en vertu du CLOUD Act ?

La plupart des types de données (y compris le contenu des communications) ne peuvent être obtenus en vertu du CLOUD Act que lorsqu'un tribunal a constaté que des conditions spécifiques sont remplies.[7]

Pour obtenir le contenu numérique, les forces de l'ordre doivent obtenir un mandat, qui est délivré par un tribunal indépendant. Ce processus est soumis à une série de garanties constitutionnelles, légales et procédurales en vertu du droit américain.

IL Y A TROIS ÉTAPES CLÉS :

1. **LA DEMANDE : Un agent des forces de l'ordre doit soumettre une demande de mandat à un tribunal indépendant.** La demande doit inclure des faits établissant que les informations recherchées contiennent des preuves d'un crime - et décrire avec précision les informations à obtenir. L'agent qui soumet la demande de mandat doit prêter serment sur ces faits.
2. **ACCORD DU TRIBUNAL : Un tribunal indépendant doit déterminer qu'il existe un motif raisonnable.** Un mandat ne peut être délivré que lorsqu'un procureur a convaincu un tribunal qu'il existe un motif raisonnable qu'un crime spécifique a été commis ou est en train de l'être et que le lieu à chercher, tel qu'un compte de messagerie, contient des preuves de ce crime spécifique. Cette constatation est faite par un tribunal indépendant et non par l'autorité répressive elle-même.
3. **POSSIBILITÉ DE CONTESTER : Une fois la demande d'accès émise, les entreprises numériques peuvent la contester et soulever des conflits juridiques.** Les entreprises numériques peuvent contester une demande d'accès devant un tribunal en déposant une motion pour modifier ou annuler l'ordonnance auprès du tribunal qui l'a émise.8 En effet, le CLOUD Act préserve spécifiquement la possibilité pour les fournisseurs d'introduire des "contestations de courtoisie" en droit commun si une demande d'accès est en conflit avec la loi d'un pays étranger.[9] Les tribunaux évaluent ces contestations en fonction d'une série de facteurs, notamment le degré de spécificité de la demande, le fait que les informations recherchées proviennent des États-Unis et le fait que les informations pourraient être obtenues par d'autres moyens.[10]

Ces exigences imposent d'importantes restrictions aux injonctions. Les fournisseurs qui transmettent du contenu numérique à une agence gouvernementale américaine en l'absence d'un mandat de perquisition conforme à ces normes s'exposent à une responsabilité civile et pénale.[11]

Les demandes d'accès peuvent viser des données provenant de fournisseurs numériques dont le siège est situé en dehors des États-Unis.

- Le CLOUD Act régit la délivrance de demande d'accès visant de nombreux types de fournisseurs numériques.[12]
- Ces derniers peuvent faire l'objet de demandes en vertu du CLOUD Act s'ils sont soumis à la juridiction américaine et ont la capacité technique d'accéder aux données recherchées, quel que soit le lieu de leur siège, où les services sont fournis et où les données stockées.[13]
- De nombreuses sociétés basées en dehors des États-Unis sont soumises à la juridiction américaine, par exemple lorsqu'une société a des opérations ou des bureaux aux États-Unis ou conclut des contrats avec des clients américains.[14]

Qu'est-ce qu'un mandat ?

Les organismes américains chargés de l'application de la loi utilisent des mandats pour obtenir du contenu numérique. Les mandats sont soumis à des garanties strictes et ne peuvent être délivrés que si un tribunal estime qu'un agent a démontré qu'il existe un motif raisonnable de croire que les informations recherchées contiennent des preuves d'un crime.

Qui délivre les mandats ? Les tribunaux délivrent les mandats. Cela garantit qu'un juge indépendant, et pas seulement les autorités qui demandent le mandat, approuve la perquisition demandée.

D'où proviennent les exigences relatives à la délivrance d'un mandat ? La Constitution, les lois et les règles de procédure des États-Unis imposent toutes des exigences en matière de protection de la vie privée applicables aux mandats. En vertu du 4ème amendement de la Constitution, les mandats ne peuvent être délivrés que (1) sur la base d'un motif raisonnable, (2) s'ils sont appuyés par un serment ou une déclaration solennelle, (3) s'ils décrivent précisément les lieux à fouiller et les objets à saisir. Les lois fédérales telles que l'ECPA limitent encore plus les situations dans lesquelles les forces de l'ordre peuvent demander un mandat. En outre, les règles fédérales de procédure pénale contiennent des garanties supplémentaires limitant la manière dont les tribunaux peuvent délivrer des mandats.

Les mandats peuvent-ils approuver la collecte en masse ? Non. Les mandats sont délivrés dans le cadre d'affaires pénales particulières, afin d'obtenir des types de données spécifiques qui sont identifiés avec précision dans le mandat lui-même. Le 4ème amendement de la Constitution exige qu'un mandat décrive avec précision le lieu à fouiller et les personnes ou objets à saisir, ce qui garantit que la recherche sera précisément adaptée à ses justifications.

LES TRIBUNAUX AMÉRICAINS : UN CONTRÔLE INDÉPENDANT

La Constitution des États-Unis fait du pouvoir judiciaire (tribunaux) l'un des trois pouvoirs séparés et distincts du gouvernement fédéral.[15] Les deux autres branches sont le pouvoir exécutif (dirigé par le président) et le pouvoir législatif (le Congrès). En vertu de cette séparation des pouvoirs, le pouvoir judiciaire ne crée pas les lois (rôle du Congrès) et ne les applique pas (rôle du Président, des départements et agences du pouvoir exécutif).[16] Cette structure garantit que les tribunaux sont des entités indépendantes, chargées d'interpréter et d'appliquer les lois de manière équitable et impartiale pour résoudre les litiges. L'indépendance du pouvoir judiciaire fédéral est ancrée dans la Constitution américaine, qui exige que les juges fédéraux soient nommés à vie.

En pratique, cela signifie que lorsqu'un organisme chargé de l'application des lois (qui fait partie du pouvoir exécutif) demande un mandat pour obtenir des informations détenues par une entreprise de technologie, cette demande de mandat est examinée par un juge indépendant qui fait partie du pouvoir judiciaire.

BRANCHE LÉGISLATIVE
Congrès—Elabore les lois

Le Congrès élabore les lois qui précisent les circonstances dans lesquelles les forces de l'ordre peuvent demander un mandat et les normes d'émission d'un mandat ; ces lois complètent les exigences constitutionnelles.

POUVOIR EXÉCUTIF
Président—Applique les lois

Les forces de l'ordre font partie du pouvoir exécutif ; elles doivent s'adresser aux tribunaux pour obtenir un mandat et doivent satisfaire les exigences imposées par les lois (adoptées par le Congrès) et par la Constitution.

POUVOIR JUDICIAIRE
Tribunaux—Interprètent les lois

Les tribunaux délivrent des mandats ; ils ne le font que lorsqu'un organisme chargé de l'application de la loi en fait la demande et remplit les conditions imposées par les lois (adoptées par le Congrès) et par la Constitution.

LE CLOUD ACT COMPORTE DEUX PARTIES

PARTIE 1

Il clarifie que les demandes d'accès dans le cadre de l'ECPA existant concernent les données quel que soit l'endroit où elles sont stockées.

PARTIE 2

Il crée un nouveau cadre pour les accords entre gouvernements sur les demandes transfrontalières d'application de la loi.

Le CLOUD Act : Une modification ciblée de la législation américaine

Le Cloud Act n'a pas créé un nouveau cadre juridique permettant aux forces de l'ordre d'obtenir des informations détenues par les entreprises numériques, mais a plutôt apporté des modifications ciblées au cadre juridique établi de longue date par l'Electronic Communications Privacy Act (ECPA).

ECPA : Promulguée en 1986, l'ECPA a été conçue pour protéger la confidentialité des communications électroniques telles que les courriels, notamment en limitant les situations dans lesquelles les forces de l'ordre peuvent obtenir des communications électroniques auprès des entreprises numériques.[17] L'ECPA a établi le cadre juridique définissant les exigences que ces autorités doivent respecter pour obtenir des informations auprès des entreprises numériques.[18]

CLOUD Act : Promulguée en 2018, le CLOUD Act a modifié l'ECPA pour préciser que le lieu de stockage des données n'est pas le facteur déterminant pour qu'un tribunal puisse délivrer un mandat via l'ECPA.[19] Par conséquent, le CLOUD Act n'a pas créé une structure juridique entièrement nouvelle en vertu de laquelle les données peuvent être obtenues par les autorités américaines, mais a plutôt clarifié la manière dont le cadre juridique de l'ECPA s'applique dans un scénario spécifique, lorsque les données recherchées ne sont pas stockées aux États-Unis.[20] En pratique, les demandes d'accès via le CLOUD Act sont toujours émises dans le cadre juridique de l'ECPA - et sont souvent appelées simplement "mandats ECPA" ou "ordonnances ECPA." Le CLOUD Act préserve aussi expressément la possibilité pour les fournisseurs de services d'introduire des "contestations de courtoisie" en droit commun si un ordre est en conflit avec une loi étrangère.[21]

Que sont les accords CLOUD Act ?

La deuxième partie du CLOUD Act crée un cadre pour de nouveaux accords de gouvernement à gouvernement afin de régir l'accès transfrontalier aux données détenues par les fournisseurs de technologies numériques. Actuellement, les organismes chargés de l'application de la loi d'un pays qui cherchent à obtenir des preuves stockées dans un autre pays utilisent le processus du traité d'entraide judiciaire (TEJ – ou *Mutual Legal Assistance Treaty/MLAT*). Le CLOUD Act définit un nouveau cadre, avec des exigences spécifiques auxquelles un pays doit satisfaire, avant que les États-Unis puissent conclure un accord au titre du CLOUD Act. Il s'agit notamment de démontrer que la législation nationale du pays offre de solides protections de fond et de procédure pour la vie privée et les libertés civiles, sur la base de facteurs énoncés dans la loi.[22] En outre, si un mandat américain entre en conflit avec le droit d'un pays tiers qui a conclu un accord au titre du CLOUD Act, la loi prévoit un mécanisme supplémentaire permettant aux entreprises technologiques de contester le mandat devant les tribunaux.[23]

En octobre 2019, les États-Unis et le Royaume-Uni ont conclu le premier accord CLOUD Act.[24] Le même mois, les États-Unis et l'Australie ont annoncé les négociations d'un autre accord CLOUD Act.[25] Les États-Unis et la Commission européenne ont également entamé des négociations officielles en vue d'un accord UE-États-Unis visant à faciliter les preuves électroniques dans les enquêtes criminelles.[26]

Références

[1] Le CLOUD Act a été adopté dans le cadre du Consolidated Appropriations Act, 2018, Pub. L. n° 115-141 (23 mars 2018), https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. Voir la division V CLOUD ACT (modifiant la loi sur la confidentialité des communications électroniques, 18 U.S.C. 2701 et seq).

[2] Idem.

[3] Voir 18 U.S.C. 2713 (ajouté à l'ECPA par la Sec. 103 du CLOUD Act).

[4] Voir 18 U.S.C. 2523.

[5] Voir 18 U.S.C. 2703(a) (nécessitant la publication de mandats pour les procédures pénales devant les courts fédérales ou d'état); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[6] Voir *Seeking Enterprise Customer Data Held by Cloud Service Providers*, U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division (December 2017), https://www.justice.gov/criminal-ccips/file/1017511/download.

[7] Sans l'approbation préalable d'un tribunal, une agence gouvernementale ne peut obtenir qu'un ensemble limité d'informations par le biais d'une assignation à comparaître, qui peut rechercher sept types spécifiques de données identifiées dans la loi, y compris le nom, l'adresse et les informations de facturation d'un abonné. 18 U.S.C. 2703(c)(2). Une ordonnance du tribunal émise sur la base d'une preuve moindre qu'un mandat peut être obtenue pour rechercher des métadonnées, telles que des données transactionnelles ; cela nécessite de démontrer que des faits articulables montrent des motifs raisonnables de croire que les informations recherchées sont pertinentes et importantes pour une enquête criminelle en cours. 18 U.S.C. 2703(d).

[8] Voir 18 U.S.C. 2703 note (2018) (Rule of Construction).

[9] Idem.

[10] Voir Restatement (Third) of Foreign Relations Law § 442. D'autres facteurs doivent être pris en compte, notamment (1) l'importance pour l'enquête ou le litige des documents ou informations demandés ; (2) la mesure dans laquelle le non-respect de la demande porterait atteinte à des intérêts importants des États-Unis, et (3) la mesure dans laquelle le respect de la demande porterait atteinte à des intérêts importants de l'État où se trouvent les informations.

[11] Voir 18 U.S.C. 2702(a)-(b) (interdisant aux fournisseurs de communications électroniques et de services de cloud de divulguer le contenu numérique sauf dans neuf circonstances spécifiques, notamment en vertu d'un mandat, avec le consentement du destinataire et si cela est nécessaire pour offrir le service).

[12] La loi CLOUD modifie l'ECPA ; les demandes d'accès émises en vertu de ces pouvoirs peuvent atteindre les fournisseurs de services de communications électroniques et les fournisseurs de services informatiques à distance. Voir 18 U.S.C. 2511(15) ; 18 U.S.C. 2711(2) (définition des fournisseurs de services informatiques à distance).

[13] Voir 18 U.S.C. 2713 (qui stipule que les demandes d'accès peuvent atteindre les informations qui sont "en possession, sous la garde ou sous le contrôle" d'un fournisseur).

[14] Une entreprise est soumise à la juridiction des États-Unis si elle a des "contacts minimums" avec les États-Unis, par exemple lorsqu'une entreprise étrangère "se prévaut délibérément" du privilège de faire des affaires aux États-Unis en servant des clients américains.

[15] Voir la Constitution des États-Unis, article III.

[16] Voir, par exemple, Administrative Office of the US Courts, Understanding the Federal Courts, https://www.uscourts.gov/sites/default/files/understanding-federal-courts.pdf.

[17] Pub. L. No. 99-508 (1986), https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf.

[18] Voir, par exemple, House Report No. 99-647 (1986), https://www.justice.gov/sites/default/files/jmd/legacy/2013/10/16/houserept-99-647-1986.pdf; et Senate Report No. 99-541 (1986), https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf.

[19] Pub. L. n° 115-141 (23 mars 2018), https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. Voir la division V, CLOUD ACt (modifiant la loi sur la confidentialité des communications électroniques, 18 U.S.C. 2701 et seq.).

[20] Voir 18 U.S.C. 2713 (ajouté à l'ECPA par le CLOUD Act).

[21] 18 U.S.C. 2703 note (2018) (Rule of Construction).

[22] 18 U.S.C. 2523(b)(1).

[23] 18 U.S.C. 2703(h)(2)(A).

[24] Voir *US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, Department of Justice, October 3, 2019, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[25] Voir *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement*, U.S. Department of Justice, October 7, 2019, https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[26] Voir *Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, Department of Justice, September 26, 2019, https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.