CLOUD Act : quelle protection pour nos données ?

Dans le contexte du CLOUD Act, « le chiffrement est votre ami », résume Dominic Trott, directeur de recherche associé chez IDC dans le domaine de la sécurité et de la vie privée.

Sa conclusion : face à l'incertitude juridique, cherchez des réponses chez vos fournisseurs technologiques. Le chiffrement en fait partie, aux côtés, entre autres, de la segmentation des données.

À l'invitation d'AWS, le cabinet d'études a entrepris de démystifier cette loi fédérale américaine applicable depuis mars 2018.

Concernés au premier chef, les prestataires de services cloud ont accentué leur communication au vu de l'incertitude que suscite le texte.

Donald Trump l'avait promulgué sur fond de litige entre l'administration américaine et Microsoft.

Ce dernier, sollicité dans une affaire de trafic de drogue, refusait de livrer des données hébergées en Irlande. Il l'avait emporté en première instance… puis devant la Cour d'appel. Celle-ci avait considéré qu'en exigeant d'un fournisseur de services basés aux États-Unis qu'il fournisse des informations localisées stockées à l'étranger, le gouvernement U.S. allait à l'encontre du principe de non-extraterritorialité de la loi.

L'affaire est remontée jusqu'à la Cour suprême, mais la procédure a tourné court avec l'adoption du CLOUD Act.

Officiellement, le texte a pour objectif de clarifier le Stored Communications Act, sur lequel Washington avait fondé sa requête à Microsoft. Et plus précisément de lui donner une dimension extraterritoriale – d'où l'acronyme CLOUD, pour « Clarifying lawful overseas use of data ».

CLOUD Act : le « court-circuit »

Des dispositifs préexistaient au CLOUD Act pour permettre aux autorités répressives américaines d'accéder à des données localisées hors des États-Unis. Notamment les lettres rogatoires, transmises entre tribunaux.

Autre mécanisme : l'entraide pénale internationale. Moyennant l'aval d'un juge indépendant, un gouvernement peut en solliciter un autre dans le cadre d'un accord d'assistance mutuelle (MLAT, pour « Mutual legal assistance treaty »). Les États-Unis ont signé de tels accords avec une soixantaine de pays.

Bien que plus rapide que les lettres rogatoires, les MLAT restent un dispositif contraignant. Les démarches **prennent en moyenne 10 mois pour aboutir**, d'après les données de l'Union européenne.

Le CLOUD Act « court-circuite » ces procédures en ouvrant la voie à des accords bilatéraux. C'est-à-dire des négociations entre pays pour lever les barrières aux réquisitions.
Aux États-Unis, par exemple, le SCA constitue le principal obstacle. De manière générale, il interdit aux entreprises soumises au droit américain de communiquer des données à des pays étrangers.

Les barrières levées, l'exécutif peut faire ses réquisitions directement auprès de deux catégories de fournisseurs. D'un côté, ceux qui procurent des « services de communications électroniques au public ». De l'autre, les « services d'informatique à distance » (les plates-formes cloud en font partie).

Les États-Unis ne peuvent solliciter que les fournisseurs soumis au droit américain. Tout n'est cependant pas clair sur ce point. Par exemple, avoir des clients sur place sans disposer d'une implantation peut-il être retenu comme critère ? Theodore Christakis, membre de l'Institut universitaire de France et du Conseil national du numérique, estime que non. Y compris quand on mentionne les doutes qu'exprime au contraire Frédéric Pierucci, l'ancien directeur d'Alstom Power.

Contrôles *a posteriori*

Le CLOUD Act impose un certain nombre de conditions pour les demandes que formulent les autorités américaines. Elles doivent notamment être ciblées, basées sur « des faits raisonnables et crédibles » ou encore ne pas menacer la liberté d'expression.

Rien n'oblige à notifier les personnes physiques ou morales que visent ces requêtes. Elles ne font par ailleurs **pas l'objet d'un contrôle *a priori***. Il appartient aux fournisseurs de services de les contester sous 14 jours devant la justice U.S. s'ils ont des raisons de croire :

- que la personne visée n'est pas citoyen ou résident permanent des États-Unis (sont considérées comme tels les associations dont « un grand nombre de membres » sont citoyens ou résidents permanents américains) ;
- qu'il existe un risque de conflit avec les lois d'un autre pays.

Pour être sollicités, les fournisseurs de services doivent avoir « la possession, le contrôle ou la responsabilité » des données recherchées.
Problème : la définition n'est pas harmonisée au niveau fédéral. Le deuxième circuit (Connecticut, New York, Vermont) en a l'une des interprétations les plus larges.

Une réponse européenne ?

Certaines dispositions du RGPD encore plus de zones d'ombre, en tout cas pour ce qui est des données personnelles.

Il faudra en tenir compte dans le cadre de l'accord bilatéral qui se dessine au niveau européen, à travers le **projet de règlement dit « e-Evidence »**, en discussion depuis 2016 après les attentats de Bruxelles.

La Commission européenne a proposé un texte en avril 2018.
L'objectif est le même qu'avec le CLOUD Act : créer un cadre juridique qui favorise l'accès transfrontière aux preuves électroniques dans le cadre de procédures pénales.

La principale mesure consiste à créer des injonctions de production et de conservation. Elles s'appliqueraient directement aux prestataires offrant des services dans l'Union et établis ou représentés dans un autre État membre, indépendamment de la localisation des données.

Le Conseil de l'Europe a arrêté sa position en décembre 2018 – et l'a précisée en mars 2019 concernant la désignation de représentants légaux pour la collecte de preuves. Il estime qu'un accord bilatéral noué avec les États-Unis sous l'égide du règlement « e-Evidence » permettrait de **ramener à 10 jours le délai de transmission des données demandées**.

L'épine RGPD

Le Parlement européen devrait arrêter sa position au mois d'octobre. Pourront alors s'engager les négociations en trilogue, avec en toile de fond les réserves exprimées notamment par le G29 (devenu le Comité européen de la protection des données). Celui-ci redoute que l'accès aux données de souscription (informations sur l'abonné à un service) constitue une ingérence dans le droit à la vie privée.

D'autres notions restent à préciser, telle celle de crime « sérieux », motif que les États-Unis peuvent avancer pour demander des données.

L'UE travaille aussi sur un protocole additionnel à la Convention de Budapest sur la cybercriminalité. Le but : établir un régime d'entraide judiciaire plus efficace entre les 63 États signataires.

Concernant le RGPD, on surveillera d'éventuels conflits avec les articles 44 et 50. Le premier pose les principes généraux du transfert de données personnelles vers des pays tiers ou à des organisations internationales. Le second traite de la coopération internationale dans le domaine.
Se pose la question de savoir si les accords bilatéraux tomberont sous le coup des dérogations mentionnées à l'article 49. Plus précisément leur nécessité « pour des motifs importants d'intérêt public ».

Photo d'illustration © Pixabay via *Pexels.com*