Le cocktail détonnant du *CLOUD Act*

Extraterritorialité, sécurité nationale et libertés individuelles

« *When a statute gives no clear indication of an Extraterritorial application, it has none.* »
Cour suprême des États-Unis, 24 juin 2010, n° 08-1191, *Morrison et al. c/ National Australia Bank Ltd. et al.*

« *Our government should accord a "decent Respect to the Opinions of Mankind".* »
Déclaration d'indépendance des États-Unis, 1776.

MARIE ABADIE
Contract Manager
Cabinet ITLaw

EMMANUEL JOUFFIN
Docteur en droit
Responsable juridique de banque

Par une disposition introduite de manière subreptice dans la plantureuse loi sur les dépenses 2018 (plus de 2 000 pages), les États-Unis ont mis en place un mécanisme original de collecte directe de communications électroniques localisées à l'étranger, dans le cadre d'enquêtes pénales. Ce dispositif suscite de nombreuses interrogations, notamment en ce qui concerne sa compatibilité avec divers textes, dont le Règlement européen relatif à la protection des données (RGPD), mais aussi au sujet de la réplique envisagée par l'Union européenne.

Le *CLOUD Act*, pour *Clarifying Lawful Overseas Use of Data Act*[1], a été promulgué par le président Trump le 26 mars 2018, soit deux mois avant l'entrée en vigueur du dispositif protecteur du RGPD[2]. Cette loi US amende la loi SCA (*Stored Communications Act*) de 1986, cette dernière fixant un principe de confidentialité et de protection des données de communication, traitées ou stockées par des fournisseurs de services de communication. On notera que le gouvernement américain a reconnu, s'agissant de ce dernier texte que « *it is undisputed that [the SCA] lacks extraterritorial reach* »[3].

Le *CLOUD Act* est une séquelle d'une affaire dans laquelle Microsoft avait refusé aux autorités US, s'agissant d'une affaire de stupéfiants, l'accès à des données stockées dans un *data center* irlandais. Microsoft avait fait valoir que le contenu des courriels, n'appartenant qu'à ses clients, n'était donc pas sous son contrôle et que le gouvernement américain avait pour obligation d'utiliser un mandat de perquisition (*warrant*), plutôt qu'une citation à comparaître, pour demander la communication du contenu des emails stockés en Irlande.

Le 14 juillet 2017, la cour d'appel de New York a donné raison à Microsoft, concluant que le gouvernement américain ne pouvait unilatéralement contraindre Microsoft à lui donner accès à des données stockées exclusivement en dehors des États-Unis et devait dès lors faire appel aux traités d'assistance judiciaire mutuelle.

Sans attendre la décision de la Cour suprême[4], saisie par le *Departement Of Justice*, le gouvernement a adopté un texte prévoyant en présence de « *serious crime* »[5], un droit de communication au bénéfice des autorités US de diverses données, sans considération du lieu où ces données sont stockées. Bien entendu, les sociétés « incorporées » aux États-Unis, et celles que ces dernières contrôlent, sont les plus directement concernées.

La raison d'être de ce texte est ainsi exprimée par le Congrès : « *L'accès en temps utile aux données électroniques détenues par les fournisseurs de service de communication est un élément essentiel des efforts du gouvernement pour protéger la sécurité publique et combattre la criminalité grave, incluant le terrorisme. Ces efforts, déployés par le gouvernement des États-Unis sont entravés par l'impossibilité d'accéder aux données stockées en*

1. « Clarifier l'usage des données hébergées à l'étranger en matière judiciaire ». V. Déclaration d'indépendance des États-Unis – 1776 *in Amicus curiae AT&T pour Microsoft*, spéc. pp. 23-27 : https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf.
2. Règlement n° 2016/679 du 27 avril 2016, JOUE n° L. 119, 4 mai 2016, p. 1.
3. https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/ATT-AmicusBrief.pdf.
4. Laquelle s'est élevée à plusieurs reprises contre l'extraterritorialité des lois US : en 2010, dans l'affaire *Morrison c/ National Australia Bank* (24 juin 2010) la Cour suprême affirme, de manière générale, un principe de droit américain de présomption contre l'extraterritorialité (*presumption against extraterritoriality*), d'où il ressort que sauf volonté explicite du Congrès, une loi n'a pas une portée extraterritoriale. *Idem*, *Kiobel c/ Royal Dutch Petroleum*, 17 avril 2013 ou bien encore, *OBB Personenverkehr AG c/ Sachs*, 1er décembre 2015. Les *amicus brief* du Parlement européen et du Conseil des barreaux européens sont disponibles aux adresses suivantes : http://bit.ly/2EclkMD (PE) et http://bit.ly/2DFlfE3 (CCBE).
5. *CLOUD Act* : Sec. 2. *Congressional findings*, *cf. infra*, § 6.

dehors des États-Unis qui sont sous la garde, le contrôle ou la possession de fournisseurs de services de communications relevant de la juridiction des États-Unis »[6]. On soulignera que le *CLOUD Act* est le fruit d'un cavalier législatif, adopté sans discussion, inclus subrepticement dans la loi de finances 2018.

Le *CLOUD Act* n'est pas le premier texte s'intéressant aux communications de données dans le domaine des enquêtes judiciaires. Côté européen, on rappellera que la Convention de La Haye du 18 mars 1970, sur l'obtention des preuves à l'étranger en matière civile ou commerciale, ratifiée par les États-Unis, aborde cette question. En matière pénale, on mentionnera également la Décision du Conseil 2016/920 du 20 mai 2016[7], dont l'objectif est de garantir un « *niveau élevé de protection des données et, partant, d'améliorer la coopération entre les parties* ».

Pour les États-Unis, on citera notamment l'*Umbrella Agreement*[8] (accord parapluie) sur la coopération judiciaire en matière pénale. Cet accord prévoit, notamment, la limitation du traitement des données personnelles aux finalités que sont la prévention, la détection, la recherche et les poursuites judiciaires, une durée de conservation des données personnelles en fonction de la finalité du traitement, ainsi que la création d'un mécanisme d'information mutuelle sur les violations de sécurité. La conformité de ce dernier accord avec la Charte des droits fondamentaux de l'Union européenne[9], théoriquement applicable à « *toute personne* » sur le territoire de l'Union européenne, indépendamment de sa nationalité ou de son statut, était fortement questionnée dans la mesure où l'accord ne s'applique qu'aux essortissants des parties audit accord.

Par ailleurs, le *Foreign Intelligence Surveillance Act* (FISA) est aussi utilisé pour des investigations liées à la sécurité nationale. Les fournisseurs de services en ligne sont sollicités sur ce fondement pour donner accès à des données de contenu et des métadonnées. À ce titre, les autorités peuvent obtenir des commissions rogatoires ou « *physical search order* » de la part de la *Foreign Intelligence Surveillance Court* (FISC) pour accéder à des courriels et, plus largement, à des données personnelles, ainsi que présenter des demandes de surveillance à l'égard de personnes situées en dehors des États-Unis (section 702 of FISA).

1. Quel est le champ d'application territoriale du *CLOUD Act* ?

Le *CLOUD Act* permet aux autorités américaines, dans le cadre d'enquêtes judiciaires criminelles, d'obtenir des données stockées en dehors des États-Unis, le § 2713 de ce texte visant « *[…] tout enregistrement ou autre information concernant un client ou un abonné en sa possession, la garde ou le contrôle, que cette communication, cet enregistrement ou d'autres informations se trouvent à l'intérieur ou à l'extérieur des États-Unis* »[10]. Ce faisant, ce texte simplifie et modifie la procédure d'accès aux informations, qui nécessitait un recours aux MLAT (*Mutual Legal Assistant Treaty*)[11], dans une démarche qui, pour les autorités américaines, ne relève pas de l'effet extraterritorial des textes.

La doctrine du gouvernement américain peut se résumer ainsi : dès lors que des données sont accessibles depuis les États-Unis, fussent-elles stockées hors de ces mêmes États-Unis, elles sont supposées se trouver « *à portée de clic* » et, par une fiction « *juridico-technique* », être sur le sol américain. Au cours de la procédure opposant Microsoft à l'État américain, ce dernier a souligné : « *Microsoft's U.S. based employees could make that disclosure without leaving their desks* »[12]. La question n'est donc pas où se trouvent les données, mais d'où sont-elles accessibles. Cette approche fait peu de cas du fait que les données transmises ont été préalablement physiquement stockées en un lieu géographique précis.

Par ailleurs, toujours pour le gouvernement américain, la prise de connaissance des données n'intervenant qu'au moment où l'agent du gouvernement prend connaissance des mails expédiés aux États-Unis, cette divulgation se déroule sur le territoire américain et par voie de conséquence, seule la loi américaine est applicable, indépendamment du lieu d'extraction des données.

La question de l'extraterritorialité du *CLOUD Act* fait l'objet d'analyses diamétralement opposées, oscillant entre dimension extraterritoriale évidente[13], et absence d'un tel effet[14]. Sans entrer dans un débat dont les termes dépassent les limites de la présente étude, on ne peut que rappeler que les serveurs sur lesquels sont stockées les données se trouvent, en principe, sur le territoire d'un État souverain identifié et que l'accès aux données s'y trouvant ne peut être la résultante exclusive d'un activisme législatif dont le but est la promotion, si ce n'est de la puissance américaine, du moins de ses intérêts.

6. « *Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism. Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications service providers that are subject to jurisdiction of the United States.* »

7. Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière : https://publications.europa.eu/fr/publication-detail/-/publication/686d63d6-2f99-11e6-b497-01aa75ed71a1/language-fr.

8. http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm. Cf. Contrôleur européen à la Protection des données, avis n° 1/2016, avis préliminaire relatif à l'accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière. L'*Umbrella Act* ne doit pas être confondue avec le *privacy shield*, lequel relève des relations commerciales.

9. Notamment ses articles 7 droit à la vie privée, 8 relatif au droit à la protection des données et 47 relatif au droit à un recours juridictionnel effectif.

10. § 2713: « *Required preservation and disclosure of communications and records.* » Le texte précise : « *[…] à propos de la communication des données: "regardless of whether such communication, record, or other information is located within or outside of the United States".* »

11. Accords d'assistance juridique mutuelle.

12. https://www.wsj.com/articles/supreme-court-to-hear-microsoft-case-on-emails-customer-data-stored-overseas-1519641001.

13. Th. Christakis The Chertoff Group, CEIS, déc. 2017, (spéc. § 12 et s) - https://ceis.eu/wp-content/uploads/2017/12/livre_blanc_FR_WEB.pdf ; « Données personnelles : Le *CLOUD Act* : pour un accès extra-territorial aux données », *Expertises*, avril 2018 ; P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières – Remarques sur l'application du droit dans l'espace numérique à la lumière du *CLOUD Act* », *Cahiers de droit de l'entreprise* n° 4, juill. 2018, dossier 28.

14. R. Bismuth, « Every Cloud Has a Silver Lining – Une analyse contextualisée de l'extraterritorialité du *CLOUD Act* », JCP E, n° 40, 4 oct. 2018, 1497, spéc. § 11 et s.

On constate en tous les cas un heurt frontal avec le RGPD pour lequel la protection des données personnelles s'applique dès lors que les activités du responsable du traitement ou du sous-traitant se déroulent « *sur le territoire de l'Union* »[15].

2. Le *CLOUD Act* peut-il conduire à une collecte massive de données ?

En janvier 2014, le président Obama a fait publier la directive présidentielle n° 28 (PPD-28)[16] encadrant les activités du renseignement américain. Cette directive prévoit que les entités du renseignement doivent être sélectives dans leurs collectes, le recours à un « chalutage » massif de données étant réservée à six domaines[17].

Depuis 2015, la loi américaine sur la liberté (*Freedom Act*[18]) restreint également la collecte massive de données et prévoit que les entreprises publient des rapports de transparence indiquant le nombre de demandes d'accès aux données émanant des pouvoirs publics. On notera toutefois que la section 702 du *Foreign Intelligence Surveillance Amendment Act* (FISA[19]) autorise les services secrets américains à collecter, sans mandat, par le biais d'entreprises américaines, des données concernant des citoyens non-américains (et uniquement ceux-là) se trouvant hors des États-Unis.

Ce dernier texte s'affranchit des limites qui devraient être posées à une surveillance constante et à grande échelle. En 2012, le Parlement européen a ainsi souligné : « *§ 1881a of FISAA for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to cloud computing* »[20]. Ce point est très sensible, notamment afin d'évaluer le degré de protection du *privacy shield*. Le 19 janvier 2018, le Président Trump a ratifié la reconduction, en l'état, de cette section 702 pour six ans. Dans un tweet, ce dernier a clairement énoncé que le renouvellement du FISA concernait la « *foreign surveillance of foreign bad guys on foreign land* ». Cet apophtegme ne s'accommode guère de la moindre exégèse.

S'agissant des données concernées, la rédaction du § 2713 du *CLOUD Act*[21], et l'emploi du mot « *contents* », volontairement vague, ne permet pas de faire une distinction entre les données concernées. Conformément aux dispositions du SCA, celles-ci peuvent être des données de contenu (substance et signification d'un message), des métadonnées (ID, logs, adresses mail) et des données de souscription concernant un abonné (tels que ses nom, prénom, adresse, numéro de téléphone, moyen de paiement, numéro de carte bancaire), notamment celles stockées dans le *cloud*[22]. L'important est que la communication de ces données semble utile ou nécessaire à l'auteur de la requête.

3. La mise en œuvre *CLOUD Act* est-elle conditionnée à un accord bilatéral ?

La signature d'un accord avec un « *qualifying foreign government* » (QFG) n'est pas une condition de mise en application du *CLOUD Act*. Par conséquent, ce dernier peut d'ores et déjà s'appliquer sur le sol français et européen. Un accord bilatéral entre les États-Unis et des États tiers (*Executive Agreement*) est en revanche l'une des deux conditions cumulatives nécessaires pour qu'un fournisseur de services puisse s'opposer à une demande de communication de données[23]. Bien entendu, l'absence d'accord bilatéral est sans incidence sur l'application du RGPD pour les données personnelles des personnes physiques.

Pour être QFG, un État devra satisfaire à un ensemble d'exigences très détaillées visées au § 2523 du *CLOUD Act* ((b) *Executive agreement requirements*), lesquelles sont satisfaites par application du RGPD. Au titre des critères permettant de soumettre au Congrès américain un accord exécutif avec un état étranger, l'*attorney general* devra fournir un certain nombre d'éléments justificatifs, portant notamment sur le niveau des garanties en matière de vie privée, de collecte de données et de respect d'un certain nombre de droits[24].

On ne manquera pas de souligner l'asymétrie entre les exigences formulées à l'endroit des pays tiers en matière de protection des données dans le cadre du *CLOUD Act* et le flou sur les garanties offertes par les autorités US dans le cadre de la mise en œuvre du *privacy shield*[25]. Par ailleurs, le périmètre des crimes pouvant faire l'objet d'une demande sous l'empire du *CLOUD Act* semble différent selon que la demande émane d'un État tiers ou des États-Unis[26].

Les demandes présentées par un État étranger doivent concerner la prévention ou la poursuite d'infraction graves, dont le terrorisme, viser une personne précise, être conformes au droit national et offrir diverses

15. Article 3-1 du RGPD. L'article 3.2 du RGPD précise qu'un prestataire hors UE qui offre ses services sur le territoire de l'UE est concerné par le dispositif protecteur du RGPD.
16. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
17. Détection et neutralisation des menaces d'espionnage, terrorisme, armes de destruction massive, menaces contre les forces armées et menaces criminelles transnationales.
18. https://www.congress.gov/bill/114th-congress/house-bill/2048.
19. *Foreign Intelligence Surveillance Act* (FISA). Loi votée en 1978, et amandée en 2008, décrivant les procédures de surveillance tant physiques qu'électronique, ainsi que la collecte d'information à l'étranger de manière directe ou indirecte.
20. *Fighting Cyber Crime and protecting privacy in the cloud*, Parlement européen, octobre 2012, spéc. p 33. Le Parlement souligne : « *The scope of surveillance was extended beyond interception of communications, to include any data in public cloud computing as well* » (Ibid.).
21. « *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 [...]* ».
22. E. Tabatabai, « The *CLOUD Act*, Explained », Cyber, Privacy & Data Innovation Alert : https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.
23. § 2713 : « *Required preservation and disclosure of communications and records" : "A provider of electronic communication service to the public or remote computing service, [...] may file a motion to modify or quash the legal process where the provider reasonably believes : "(i) that the customer or subscriber is not a United States person and does not reside in the United States ; and "(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.* »
24. Notamment le respect de l'état de droit et du principe de non-discrimination, le respect des droits de l'homme, la protection contre les interceptions arbitraires ; le droit à un procès équitable ; la prohibition des arrestations arbitraires ; la prohibition de la torture ; des règles claires d'accès judiciaire aux données…
25. Accord entre l´UE et les États-Unis adopté par la Commission européenne le 12 juillet 2016 remplaçant le *Safe Harbour*. Le *privacy shield* prévoit que les données relatives aux citoyens européens stockées sur le territoire des États-Unis doivent bénéficier d´une protection équivalente à celle prévue par la législation européenne.
26. Cf. *infra*, § 6. « Quels types de crimes peuvent donner lieu à application du *CLOUD Act* ? ».

garanties, dont notamment une voie de contestation et la démonstration de l'existence de moyens moins intrusifs d'accès aux données. Cette dernière exigence de proportionnalité devrait valoir s'agissant des demandes présentées par les USA au titre du *CLOUD Act*.

4. Quelles sont les sociétés soumises au *CLOUD Act* ?

La rédaction du § 2713 du *CLOUD Act* est compréhensive en ce qu'elle vise les « *providers of electronic communications services or remote computing services* »[27] et vise les données qui sont en dehors des États-Unis et « *in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States* ». Aucune limitation ne permet de restreindre l'emprise du CLOUD Act aux seules entreprises américaines traitant ou hébergeant des données hors du territoire des États-Unis. Si ce texte est directement le fruit d'un refus de Microsoft de déférer à une demande de communication de données, rien ne permet d'exclure des entités autres qu'américaines.

Bien entendu, les données traitées ou hébergées chez un prestataire américain (maison mère située aux États-Unis : Google, Amazon, Microsoft, Microsoft, Salesforce, IBM…) opérant sur le sol européen sont les plus directement concernés par le *CLOUD Act*. Toutefois, des demandes pourraient être adressées à une filiale américaine d'un fournisseur français dont les données sont stockées en France. La question sera de savoir si cette filiale a les « *possession, custody or control of the information, regardless of location of data servers* »[28].

Par ailleurs, ainsi que le fait remarquer un auteur, le fait qu'une « *entreprise non américaine offre depuis l'étranger des services électroniques ciblés vers le marché américain (par exemple en ayant recours à de la publicité sur des sites américains […] les autorités pourraient la considérer comme étant "within the United States"* »[29]. On peut redouter que la détermination du périmètre de ce texte se fasse sur le fondement de décisions rendues par les juridictions US selon des critères pouvant relever d'une logique davantage économique que juridique. Le simple fait qu'un site Internet soit accessible depuis les États-Unis suffira-t-il ou bien faudra-t-il que ce dernier invite à la conclusion de contrats à distance et, cumulativement, qu'un contrat ait effectivement été conclu à distance[30] ?

Enfin, on ne peut exclure que, dans certains cas, qu'aux règles d'application du *CLOUD Act*, ne s'ajoutent celles applicables en matière de délits financiers, domaine dans lequel la compensation aux États-Unis des transactions bancaires en dollars suffit à soumettre aux lois américaines les transactions donnant lieu à ladite compensation.

5. Quelles sont les personnes visées par les demandes de renseignement du *CLOUD Act* ?

En principe, les *US persons* devraient être les seules concernées. En pratique les choses sont différentes. Dans un premier temps, toutes les personnes, et pas uniquement les « US *persons* » telles que définies par le *CLOUD Act*[31], peuvent être visées. La prise en considération de la nationalité de la personne visée par la demande de communication n'intervient que dans un second temps, à titre d'exception pourrait-on dire, lors de la contestation que peut soulever le prestataire[32]. Ainsi, le *CLOUD Act* peut concerner les données de personnes physiques, peu importe qu'elles soient ou non de nationalité américaine ou qu'elles résident ou pas sur le territoire de États-Unis.

On soulignera que les pays ayant signé un accord de réciprocité au titre du *CLOUD Act* devront, au titre de leur requête « *(ii) shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order* »[33]. Il serait surprenant que les demandes issues des États-Unis ne soient pas soumises au même devoir de précision, permettant aux prestataires concernés de réagir immédiatement au sujet de l'existence d'un critère d'américanité au sens du *CLOUD Act*. Une fois encore, la question est celle de la prévention de collecte massive de données.

6. Quels types de crimes peuvent donner lieu à application du *CLOUD Act* ?

Le *CLOUD Act* vise, dans sa section 2, les efforts du gouvernement pour protéger la « *public safety* » et combattre les « *serious crime, including terrorism* ». On notera par ailleurs que, dans le reste du texte, la notion de « *serious crime* » n'apparaît plus que s'agissant des demandes de communication tournées vers les États-Unis[34]. Il s'ensuit que les autorités US pourraient adresser des demandes de communication au sujet d'infractions très variées, relevant de la notion floue « sécurité publique ».

---

27. Définis par l'*Electronic Communications Privacy Act* de 1986 ; cf. l'*United States Code*, titre 18, § 2510(12) et 2711(2). Concerne les opérateurs de communications électroniques dont l'offre d'accès wifi publics, mais aussi les opérateurs des *cloud computing*.

28. https://fas.org/sgp/crs/misc/LSB10125.pdf.

29. CFR § 515.329(d) et 31 C.F.R. § 515.330(a)(2) cité par R. Bismuth in, « Every Cloud Has a Silver Lining – Une analyse contextualisée de l'extraterritorialité du *CLOUD Act* », JCP E, n° 40, 4 oct. 2018, 1497, spéc. § 25.

30. On retrouve ici, *mutatis mutandis*, la problématique soulevée par l'article 15, paragraphe 1, c), du règlement n° 44/2001 du 22 décembre 2001 (dit Règlement Bruxelles I) permettant de soumettre aux tribunaux de l'État membre dans lequel est domicilié le consommateur tout litige de consommation dès lors que le commerçant cocontractant a « dirigé » son activité vers ledit État.

31. « § 2523. *Executive agreements on access to data by foreign governments - '(a)* DEFINITIONS.—*In this section : "'US person' means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an un incorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States".* »

32. § 2713 (h) (2) (A) du CLOUD Act : « *A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes*
"(i) that the customer or subscriber is not a United States person and does not reside in the United States ; and
"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government ».

33. « § 2523. *Executive agreements on access to data by foreign governments - D) an order issued by the foreign government.* »

34. Cf. section 5-3-D et les commentaires de P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières. – Remarques sur l'application du droit dans l'espace numérique à la lumière du *CLOUD Act* », *Cahiers de droit de l'entreprise*, juill. 2018.

En ce qui concerne les *serious crimes*, si le code fédéral (18 USC 2703[35]) précise que les requêtes des autorités gouvernementales ne peuvent se faire que dans le cadre de la procédure criminelle prévue par ce code, le *CLOUD Act* vise spécifiquement les « *serious crime, including terrorism* »[36], ainsi que la notion de « *threat of death or serious bodily harm to any person* »[37]. La question qui se pose est celle du périmètre de ces *serious crimes*. À titre d'exemple, l'article 37 du CFR (*United States Code of Federal Regulations*) donne la définition suivante :

« *Any criminal offense classified as a felony*[38] *under the laws of the United States, any state or any foreign country where the crime occurred ; or*

Any crime a necessary element of which, as determined by the statutory or common law definition of such crime in the jurisdiction where the crime occurred, includes interference with the administration of justice, false swearing, misrepresentation, fraud, willful failure to file income tax returns, deceit, bribery, extortion, misappropriation, theft, or an attempt or a conspiracy or solicitation of another to commit a serious crime. »

On constate que cette énumération renvoie aux droits nationaux et mélange des infractions de toutes natures, celles-ci allant au-delà du cadre déterminé par la Convention de Budapest relative à la cybercriminalité du 23 novembre 2001[39]. On ne peut exclure que le *CLOUD Act* puisse être utilisé, dans le domaine des infractions économiques, afin de contourner la Convention de La Haye[40] en matière d'enquêtes civiles et commerciales. Ce dernier texte prévoit le recours à des commissions rogatoires internationales exposant les questions à poser aux personnes à entendre ou les faits sur lesquels elles doivent être entendues ainsi que les documents ou autres objets à examiner.

7. Procédure de demande d'accès à des données personnelles par le Gouvernement américain

Conformément aux dispositions du SCA, aujourd'hui le Gouvernement américain peut accéder, via trois types de procédure, aux données stockées aux États-Unis ou à l'étranger. Par le biais d'un mandat de perquisition (*warrant*), d'un *court order*, ou bien encore, de citations à comparaître (*subpoenas*).

On comprend que la dernière voie est difficilement applicable en pratique. En revanche, la première sera appliquée quand le Gouvernement, ou toute autorité de l'exécutif, souhaitera éviter la notification d'une demande d'accès auprès de l'intéressé ou de l'abonné, ce qui est souvent le cas dans les affaires criminelles. Cette procédure est plus lourde que les autres car requiert la démonstration d'une présomption sérieuse d'infraction devant un « *independant magistate* ».

Par ailleurs, les seconde et troisième voies ne sont possibles que si le Gouvernement adresse une demande au préalable à l'intéressé ou l'abonné pour obtenir des informations de base telles que susvisées précédemment. On souligne que, dans un arrêt du 22 juin 2018 [41], la Cour suprême des États-Unis a reconnu qu'un mandat de perquisition était nécessaire s'agissant de métadonnées et que la personne devait bénéficier de la protection du Quatrième Amendement de la Déclaration des Droits aux États-Unis. Ce dernier donne des garanties de droit s'agissant des perquisitions et saisies non motivées de données appartenant à une personne, localisées dans un téléphone mobile, ce dernier étant assimilé à un domicile depuis une jurisprudence de 2014.

8. Quelles voies de recours pour un fournisseur en présence d'une demande ?

Le fournisseur de services dispose d'une faculté de présenter une requête en modification ou annulation de la demande de communication d'informations. Selon le § 2713 (h) (2) (A) al. 2 du *CLOUD Act*, cette requête doit être introduite dans les 14 jours de la réception de la demande. Le recours, présenté devant une juridiction US dans les conditions fixées au « *§ 2713 - Required preservation and disclosure of communications and records* »[42], n'est recevable que si deux conditions cumulatives sont réunies : « *the required disclosure would cause the provider to violate the laws of a qualifying foreign government* » et « *the customer or subscriber is not a United States person and does not reside in the United States* »[43].

S'agissant de la première condition, pour obtenir la qualification de *qualifying foreign government*, il faut être signataire d'un *executive agreement*[44] avec les États-Unis et offrir des garanties légales similaires à celles des lois américaines s'agissant de la protection des données. La France n'a, à ce jour, pas signé d'accord avec les États-Unis. Un tel accord bilatéral devrait évidemment au préalable être également entériné par le Congrès pour entrer en vigueur. En attendant, il va être difficile à une filiale des GAFAM de résister à des demandes de communication présentées sous l'égide du *CLOUD Act* en l'absence d'accord, autrement que par un argument en défense contre un « *contempt of court* », comme l'a fait Microsoft en 2014 au regard de la requête qui lui avait été faite de fournir des contenus de courriels localisés en Irlande[45]. On imagine très lourde et couteuse l'entrée en résistance

35. L'*United States Code* constitue l'équivalent de notre Code pénal et de notre Code de procédure pénale réunis. Il comprend un chapitre 121 connu sous le nom de *Stored Communications Act* (SCA).

36. « § 2523. Executive agreements on access to data by foreign governments - Definitions. In this section, spéc. D ».

37. *Ibid.*, G.

38. De manière générale, infraction passible d'une peine d'emprisonnement supérieure à un an.

39. Dont la finalité est la lutte contre les délits informatiques, commis sur Internet ou qui ont utilisé des outils numériques, qu'il s'agisse d'infractions portant atteinte aux droits d'auteur, de fraude informatique, de pornographie enfantine ou bien encore, d'infractions liées à la sécurité des réseaux.

40. Convention du 18 mars 1970 sur l'obtention des preuves à l'étranger en matière civile ou commerciale – Art 3.

41. http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/

42. Spéc. (2) *Motions to quash or modify*.

43. « *La divulgation requise conduirait le fournisseur à violer les lois d'un gouvernement étranger qualifié ; le client ou l'abonné n'est pas une personne des États-Unis et ne réside pas aux États-Unis.* »

44. § 2523 (b) of the *CLOUD Act*.

45. https://www.datacenterdynamics.com/news/microsoft-held-in-contempt-over-dublin-emails/.

contre l'ensemble des requêtes qui sont faites à des fournisseurs dont les données sont stockées dans des pays qui n'ont pas signé d'accord.

Dans cette équation délicate, devront être prises en compte des notions particulièrement vagues telles que les « *Interests of the United States* » ou bien encore « [...] *the importance to the investigation of the information required* »...) [46].

On notera que le risque auquel s'expose le prestataire qui, se pliant au *CLOUD Act*, violerait le droit d'un QFG, ne doit pas être uniquement théorique. En effet, il est prévu que le tribunal en charge de statuer sur une requête en annulation doit prendre en compte la probabilité de la sanction à laquelle ledit prestataire s'expose [47] : « *The court shall take into account, as appropriate... the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider* ».

On soulignera qu'au moment de trancher le recours, un troisième critère est pris en compte en sus de la violation du droit d'un « *qualifying foreign government* » et du statut de non US person, à savoir : si l'ensemble des circonstances et les intérêts de la justice exigent que la demande de divulgation soit modifiée ou annulée.

En l'absence d'executive agreement avec les États-Unis, il faudra alors recourir aux « *common law standards governing the availability or application of comity analysis* » [48] c'est-à-dire, à la « courtoisie internationale » liée aux intérêts respectifs des États-Unis et de l'État où sont localisées les données, de l'importance et l'effectivité du risque contentieux qui pèse sur le fournisseur de services s'il exécute l'injonction (cf. infra, 9.b.) et des liens tant du fournisseur de services que du titulaire des données avec les États-Unis ou encore à la possibilité d'accéder à ces données par d'autres moyens [49].

La question qui se pose est bien entendu celle de la légitimité d'entreprises privées à arbitrer l'opportunité d'introduire des demandes de modification et d'annulation de requêtes gouvernementales et ce, au regard d'impératifs essentiellement économiques. Exercice délicat mettant en balance la confiance des clients avec les risques de sanctions encourues, non seulement cas de défaut de réponses aux demandes gouvernementales, mais aussi en cas d'atteintes aux données personnelles desdits clients.

9. Quelles sont les dispositions légales françaises pouvant être invoquées ?

a. RGPD

Le RGPD (art. 3) s'applique, indépendamment de la question du lieu où s'exerce le traitement et de la nationalité du titulaire des données, à toute personne se trouvant sur le territoire de l'UE. Ainsi, un touriste ou un étudiant américain est protégé par le RGPD lorsqu'il séjourne en France, indépendamment de sa nationalité ou de son lieu de résidence, critères qui sont ceux du *CLOUD Act*.

Ce dernier est donc en contradiction avec le RGPD dont l'article 48, relatif aux « *Transferts ou divulgations non autorisés par le droit de l'Union* », conditionne ces derniers à la présence « *d'un accord international, tel qu'un traité d'entraide judiciaire* » [50]. En l'absence, à ce jour du moins, d'un accord bilatéral, il est tentant de se référer à l'article 49 d) du RGPD, lequel vise « *un motif d'intérêt public* » permettant un transfert en l'absence de décision d'adéquation, ou de garanties appropriées, y compris de règles d'entreprise contraignantes. Si la lutte contre les *serious crimes* est bien d'intérêt public, il ne faut pas lire cette exception de manière extensive.

Tout d'abord, le considérant 115 du RGPD souligne que l'application extraterritoriale de lois, règlements et autres actes « *peut être contraire au droit international et faire obstacle à la protection des personnes physiques garantie dans l'Union par le présent règlement. Les transferts ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies* ». Sont ici visées des garanties suffisantes relatives à la protection des données personnelles.

Par ailleurs, ce même considérant vise une divulgation nécessaire « *pour un motif important d'intérêt public reconnu par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis* ». Toutefois cette exception, qui est celle de l'article 49 d), ne vaut que s'agissant des intérêts publics d'un des États membres de l'Union ou de l'Union elle-même [51]. On remarquera que le CEPD [52] souligne que l'existence d'un accord ou d'une convention internationale prévoyant une coopération pour favoriser cet objectif « *peut constituer un indicateur pour évaluer l'existence d'un intérêt public conformément à l'article 49, paragraphe 1, point d)* ». Il ne s'agit donc que d'un indicateur, point de départ d'une évaluation, et non d'un élément valant, per se, blanc-seing automatique aux fins de transferts de données vers des pays tiers.

La question qui se pose est simple : un accord passé dans le cadre du *CLOUD Act* assurera-t-il un niveau de protection des données personnelles plus élevé que celui que tente d'offrir le *privacy shield* dans le domaine des échanges commerciaux ? On rappellera que le 16 septembre 2016, une demande en annulation [53] de la décision d'exécution

46. § 2713. *Required preservation and disclosure of communications and records.*

47. « *Le tribunal doit prendre ne compte, le cas échéant : [...] La probabilité, l'étendue et la nature de les pénalités infligées au fournisseur ou à tout employé du fournisseur en raison d'exigences légales incohérentes imposées au fournisseur.* » *CLOUD Act* Section 2703 h) Comity analysis and disclosure of information regarding legal process contents of wire or electronic communication, « (2) ii. *Cette disposition rend délicat le fait de soulever l'argument de la loi dite de blocage* », cf. *infra* § 9 b.

48. *CLOUD Act*, section 6.

49. *CLOUD Act*, section 3, b.

50. « *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.* »

51. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* publiées le 25 mai 2018, issues du Comité européen de la protection des données (remplaçant du G29). Spéc. p. 10, § 2.4 : « *According to Article 49 (4), only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation* ».

52. *Ibid.*

53. Telle que prévue par l'article 263 du TFUE, la Cour de justice de l'Union européenne pouvant invalider la décision d'exécution (UE) 2016/1250 comme elle l'avait fait pour

2016/1250 du 12 juillet 2016 de la Commission relative à l'adéquation de la protection assurée par le *privacy shield* a été déposée par le « *Digital Right Ireland* », groupe irlandais de défense de la vie privée sur Internet[54].

Ces recours constatent que la surveillance de masse par le renseignement US perdure et s'interrogent sur l'effectivité de la protection accordée par la loi américaine pour les citoyens européens dont les données à caractère personnel sont transférées aux États-Unis. Ce constat a conduit le Parlement européen a adopté une résolution demandant à la Commission de suspendre l'accord transatlantique des flux de données si les États-Unis ne se mettent pas en conformité au premier septembre 2018[55].

On rappellera enfin que l'article 83.5 du RGPD prévoit que les violations des dispositions des articles 44 à 49 sont passibles d'amendes administratives pouvant s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Ce qui est certain, c'est qu'en l'absence d'accord bilatéral, les entreprises, dont notamment les GAFAM, sont placés en position d'arbitre avec le risque non négligeable d'être sanctionnés par les États-Unis pour ne pas avoir donné suite à une demande de communications de données ou, par l'Europe, au titre du RGPD.

b. La loi dite de « blocage »[56]

La loi n° 68-678 du 26 juillet 1968 est relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères. Cette loi interdit aux nationaux français, résidents habituels, ou à toute personne morale ayant son siège ou un établissement en France, de communiquer à des autorités publiques étrangères « *des documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin* » (article 1).

Par ailleurs, l'article 1 *bis* interdit à toute personne de demander, de rechercher ou de communiquer des informations d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci. Les personnes assujetties ont l'obligation, face à pareilles demandes, d'informer sans délai le Ministre des affaires étrangères, une sanction pénale de six mois d'emprisonnement et 18 000 euros d'amende (90 000 euros pour une personne morale)[57] sanctionnant la méconnaissance des interdictions formulées aux articles 1 et 1 *bis*.

Toutefois, le recours à la loi de blocage semble délicat[58]. La Cour suprême a en effet jugé en 1987[59], que la loi de blocage ne privait pas une juridiction américaine du pouvoir d'enjoindre la production de preuves, dans la mesure où l'expérience des tribunaux américains démontrait que le risque que les sanctions prévues par la loi française soient prononcées, était trop faible pour faire obstacle à l'application des règles fédérales américaines de procédure civile[60]. On ne connaît qu'un cas d'application de cette sanction pour un montant de 10 000 €[61], les hypothèses de mise en œuvre du « blocage » restant peu nombreuses[62].

On peut craindre que la faible fréquence, et la modicité de la sanction, soient considérées comme non significatifs par la juridiction qui aura à statuer au sujet de l'estimation du risque auquel s'expose un prestataire US soumis au *CLOUD Act*. On notera que faire le pari d'un accroissement drastique des sanctions ne constitue pas la garantie d'une plus grande efficience de la loi de blocage.

c. Directive sur la protection du secret des affaires

En sus du secret bancaire, il est possible d'invoquer la Directive n° 2016/943, transposée par la loi n° 2018-670 du 30 juillet 2018. Selon l'article 151-1 du Code de commerce, est protégée, au titre du secret des affaires, toute information répondant aux critères suivants :

– ne pas être, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;

– revêtir une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;

– faire l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret.

L'article 151-4 du Code de commerce précise qu'est illicite l'obtention d'un secret des affaires lorsqu'elle résulte soit d'un « *accès non autorisé à tout document, objet, matériau, substance ou fichier numérique qui contient le secret ou dont il peut être déduit, ou bien d'une appropriation ou d'une copie non auto-*

le *Safe Harbour* dans sa décision 8 avril 2014.

54. En décembre 2016, un recours a été déposé par la Quadrature du Nat, la French Data Network et la Fédération FDN.

55. Le président du Comité des libertés civiles estime que le *privacy shield* « *sous sa forme actuelle ne fournit pas le niveau adéquat de protection requis par la législation de protection de données européenne et la Charte de l'Union européenne [...] ne suffit pas à assurer la sécurité juridique requise pour le transfert de données à caractère personnel* » : http://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps.

56. Il existe également un règlement européen dit de blocage n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers. Ce règlement était une opposition à la loi d'Amato-Kennedy adoptée par le Congrès US le 8 août 1996 afin de sanctionner les investissements étrangers supérieurs à 20 millions de dollars par an effectués dans le secteur énergétique en Iran et en Libye.

57. Article 3.

58. Cf. *supra*, § 8 (« ...*likehood, extent and nature of penalties*... »).

59. *Société nationale industrielle aérospatiale c/ United States District Court for the southern District of Iowa*, 15 juin 1987, 482 U.S. 522 -1987.

60. Cf. *Adidas (Canada) Ltd c/ SS Seatrain Bennington*, WL 423 (SDNY, 30 mai 1984), et *Vivendi Universal*, WL 3378115 (SDNY, 16 novembre 2006).

61. Cass. crim 12 décembre 2007 pourvoi n° 07-83.228 *Christopher X*, rejet du pourvoi contre CA Paris, 9e ch., sect. B, 28 mars 2007, A. : Comm. com. électr. 2008, comm. 14.

62. Notamment : CA Versailles 16 mai 2001, *JCP* E 2007, 2330. La Cour confirme le refus d'ordonner la communication de documents économiques par la société Renault à une société étrangère en se fondant notamment sur la loi de blocage. T. com. Paris, 20 juillet 2005, *Juris-Data* n° 2005-288978. La demande de communication d'un juge américain a été jugée contraire à l'ordre public économique et financier, puisqu'elle se heurtait notamment à l'article 1er *bis* de la loi de blocage.

risée de ces éléments », soit encore qu'elle procède de « *tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale* ».

Si l'article 151-7 vise, au titre des exceptions, l'utilisation ou la divulgation du secret « *requise ou autorisée par le droit de l'Union européenne, les traités ou accords internationaux en vigueur ou le droit national, notamment dans l'exercice des pouvoirs d'enquête, de contrôle, d'autorisation ou de sanction des autorités juridictionnelles ou administratives* », au cas d'espèce et à ce jour, aucun acte bilatéral que ce soit entre la France ou les États-Unis, ou plus largement, entre l'UE et les États-Unis n'a été signé. L'article 152-6 du Code de commerce prévoit des dommages et intérêts en cas de violation de ce secret.

Dès lors, pour autant que la demande présentée sous couvert du *CLOUD Act* porte atteinte à une information couverte par l'article 151-1 du Code de commerce, cette demande sera en conflit avec le droit français. Reste à savoir si la sanction sera estimée suffisamment dissuasive par un juge US pour que ce dernier la prenne en considération (cf. *supra* en ce qui concerne la loi dite « de blocage »). Il convient de souligner que la collecte de renseignements commerciaux ou de secrets commerciaux est directement visée par la PPD28[63] dans les hypothèses où cette collecte a pour objet de protéger la sécurité nationale des États-Unis ou de leurs partenaires et alliés. Ce texte poursuit en soulignant que pareille collecte ne doit pas avoir pour objet de procurer un avantage concurrentiel aux entreprises américaines.

10. Recours au *Judicial Redress Act* pour les titulaires de données visées par une demande ?

Le Congrès américain a adopté le 24 février 2016 le *Judicial Redress Act* (JRA)[64], accordant aux ressortissants européens notamment, le droit d'introduire un recours juridictionnel aux États-Unis en cas de violation du *Privacy Act*[65] de 1974 afin de réclamer uniquement des dommages et intérêts et non des sanctions pénales (comme c'est le cas pour des citoyens américains) en cas de violation de leurs droits. Le JRA ne concerne pas la collecte de masse que l'Europe redoute.

Par ailleurs, on remarquera que l'arsenal américain sur la protection des données personnelles des citoyens US est très limité. Le *Privacy Act* permet aux agences fédérales de priver un citoyen de ses droits d'accès et de modification pour toute affaire qui ferait l'objet d'une décision de l'Exécutif ayant pour objet de conserver confidentielles des informations pour des raisons relatives au secret-défense ou à la politique étrangère.

On soulignera enfin qu'un *executive order* (décret présidentiel) du 25 janvier 2017[66] intitulé « *Executive order on Enhancing Public Safety in the Interior of the United States* » exclut les Non-Américains du *Privacy Act* : « *Les agences de sécurité devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données excluent les personnes qui ne sont pas des citoyens des États-Unis ou des résidents permanents légaux des protections du* Privacy Act » (section 14). Certes, cet *executive order* s'applique « *dans la mesure permise par la loi en vigueur* » (section 18) or, le *Judicial Redress Act* étant issu du Congrès il ne peut, en principe, être remis en cause par un « simple » décret présidentiel. Le doute est toutefois largement permis sur ce que sera la pratique en la matière.

11. Quelles mesures prophylactiques ?

On pense aux clauses contractuelles types permettant le transfert de données hors UE[67] et aux règles contraignantes d'entreprises (*Binding Corporate Rules*). Mais constituent-elles des garanties suffisantes ? Les demandes de renseignements se présenteront, non pas dans le cadre des échanges commerciaux habituels, mais dans celui d'une procédure pénale, avec un degré de pression sur le destinataire bien différent.

En pratique, dans l'attente d'un accord avec le gouvernement US, les contrats avec les prestataires US pourraient contenir une clause par laquelle ces derniers s'engagent à former opposition aux demandes des autorités américaines, conformément au § 2713 (h) (2) (A) du *CLOUD Act*, s'agissant des demandes ne concernant pas une *US person*. Ceci devrait s'accompagner d'une information sans délai du responsable de traitement de toute demande de communication de donnée présentée sous le visa du *CLOUD Act*, ce dernier devant bien entendre préserver la confidentialité de l'information.

La DGSI, en septembre 2017, a adopté une position extrême afin d'éviter les risques d'ingérence économique : « *Préférer des prestataires français, ou à défaut européens, dont les serveurs sont situés dans l'Hexagone ou dans un pays membre de l'Union européenne* »[68]. S'agissant du *cloud computing*, le *CLOUD Act* ne fait que souligner les difficultés que rencontrent les entreprises y ayant recours[69] dans le domaine de la maitrise des données qui s'y trouvent. Selon une étude de 2018[70], seulement 44 % des entreprises ont une visibilité sur le partage externe de leurs données dans le *cloud*, y compris d'éventuelles pertes de données. 78 % ont une connaissance des utilisateurs et de leurs connexions, 58 % sur les fichiers téléchargés et 56 % sur les fichiers uploadés. Enfin, 11 % ne disposent

63. Section 1. Principles Governing the Collection of Signals Intelligence.

64. https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

65. Loi encadrant la collecte, la conservation, l'utilisation et la diffusion des données personnelles par les agences américaines. Cette loi prévoit notamment la publication des traitements sur un registre fédéral, la prohibition de la divulgation des données sans le consentement écrit de la personne et offre aux personnes un droit d'accès et de modification.

66. https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

67. Déc. n °2010/87/UE de la Commission, 5 février 2010 et article 46 b du RGPD.

68. Ministère de l'Intérieur, Flash ingérence économique, spéc. p. 17 : https://www.economie.gouv.fr/files/dgsi-special-cybersecurite.pdf.

69. 97 % des entreprises utilisent des services CLOUD : étude « Navigating a Cloudy Sky : Practical Guidance and the State of Cloud Security » réalisée par l'éditeur McAfee. Cette analyse est fondée sur une enquête conduite auprès de 1 400 professionnels, d'entreprises et d'organisations commerciales situées en Australie, au Brésil, au Canada, en France, en Allemagne, en Inde, au Japon, au Mexique, à Singapour, au Royaume-Uni et aux États-Unis.

70. Étude « Cloud hard 2018 - Security with a Vengeance » conduite par Bitglass, éditeur d'un « *Cloud access Security Broker* » (CASB, *broker* d'accès sécurisé au *cloud*), fondée sur une enquête conduite auprès de 570 spécialistes de la cybersécurité et responsables informatique.

d'aucun contrôle des terminaux mobiles se connectant.

L'ACPR, dans un document de juillet 2013 intitulé « *Les risques associés au* cloud computing » énonce, parmi les mesures techniques de sécurité, le chiffrement systématique des données[71], solution qui pose la question de son coût et de son efficacité réelle face aux moyens technologiques dont disposent les agences gouvernementales US. On relèvera que la section 702 (h) de la loi FISA prévoit que le procureur général et le directeur du renseignement national peuvent ordonner à un fournisseur de services de communications électroniques, de communiquer toutes les informations ou l'assistance nécessaire pour acquérir des informations. Cette assistance pourrait concerner le forçage du chiffrement[72].

L'EBA, dans un document « *sur l'externalisation vers des fournisseurs de services en nuage* »[73] précise : « *Conformément à l'orientation 8, paragraphe 2, point e), des orientations du CECB, le contrat d'externalisation devrait obliger le fournisseur de services externes à protéger la confidentialité des informations transmises par l'établissement financier* »[74]. L'établissement devrait également non seulement « *définir et décider d'un niveau approprié de protection de la confidentialité des données, de continuité des activités externalisées* [...] »[75], mais aussi « *veiller à disposer d'un accord écrit avec le fournisseur de services en nuage dans lequel figurent notamment les obligations qui incombent à ce dernier en vertu du paragraphe 16 [assurer un niveau approprié de protection de la confidentialité]* ». Dans le contexte du *CLOUD Act*, les exigences de l'EBA devraient conduire à un renforcement de la coopération des établissements financiers avec leurs opérateurs.

12. Quelle réaction de l'Europe ?

Le 17 avril 2018, la Commission européenne[76] a présenté un projet de Règlement E-evidence « *visant à permettre aux autorités policières et judiciaires d'obtenir plus facilement et plus rapidement les preuves électroniques, comme les courriels ou les documents se trouvant sur le cloud, dont elles ont besoin pour mener à bien leurs enquêtes, ainsi que pour poursuivre et condamner les criminels et les terroristes* ». Ce règlement viendrait en lieu et place de la directive n° 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale laquelle, notamment faute de transposition uniforme, a montré ses limites. Ce règlement conduira, notamment, à la mise en place d'une injonction européenne de production permettant à une autorité judiciaire d'un État membre de demander des preuves électroniques directement auprès d'un prestataire offrant des services dans l'Union, indépendamment de la localisation des données.

Cette proposition de Règlement a suscité des réactions du G29 lequel, dans sa déclaration du 29 novembre 2017, a rappelé que l'accès des autorités aux données et métadonnées était une ingérence dans le droit à la vie privée prévue à l'article 7 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à la protection des données personnelles prévue à l'article 8 de cette même Charte. Face à cette remarque, Mme Jourová, commissaire européenne chargée de la justice, des consommateurs et de l'égalité des genres a souligné : « *Alors que les autorités répressives continuent à pâtir de la lourdeur de leurs méthodes de travail, les criminels utilisent des technologies rapides et avancées pour sévir. Il y a lieu de doter les autorités répressives de méthodes du XXIe siècle pour qu'elles puissent s'attaquer à la criminalité, tout comme les criminels recourent à des méthodes du XXIe siècle pour commettre leurs forfaits*[77]. »

Le G29 dans sa Déclaration commune du 25 novembre 2014[78] (art. 2) énonçait : « *Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux, notamment la prohibition de toute discrimination et la liberté d'expression, qui sont de valeur égale dans toute société démocratique. Ils doivent également être articulés avec l'impératif de sécurité* ». Sous la pression conjuguée de progrès technologiques, permettant une surveillance aussi étroite qu'insidieuse, et de la montée des menaces terroristes, le débat est plus que jamais celui de cette « articulation » dont l'enjeu est majeur : éviter que les démocraties, afin de défendre les valeurs qui sont les leurs, ne soient contraintes de se renier. La Commission nationale consultative des droits de l'homme (CNCDH) a exprimé très clairement ses craintes à ce sujet : « *La plus grande victoire du terrorisme serait de mettre en péril l'État de droit* »[79].

Pour conclure provisoirement, cette citation du Premier Vice-Président de la Commission européenne évoquant le règlement e-evidence : « *Les propositions présentées visent non seulement à mettre en place des nouveaux instruments qui permettront aux autorités compétentes de recueillir des preuves électroniques rapidement et efficacement par-delà les frontières mais aussi à assurer des garanties solides pour les droits et libertés de toutes les personnes concernées* ». Ces mots auraient pu être ceux d'un responsable d'une agence de renseignement US.

Le *CLOUD Act* démontre deux choses. D'une part, la difficulté grandissante à identifier la règle de droit, en présence de « *textes élaborés directement en considération de données sociologiques, d'intérêts économiques ou de résultats purement matériels* »[80], inspirés uniquement par l'instauration de rapports de force. D'autre part, on peut craindre que le grief principal que les Européens adressent à ce *CLOUD Act* soit uniquement d'avoir précédé le règlement e-evidence, lequel devrait produire des effets analogues[81]. De

71. Également évoqué par la CNIL dans ses « Recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud computing* ».
72. On se souviendra que le FBI a pu casser le code de protection des *smartphones* Apple dans le cadre d'une enquête relative à la fusillade de San Bernardino : *Les Échos*, 13 avril 2016.
73. EBA/REC/2017/03, 28 mars 2018.
74. § 4.5-15 des lignes directrices.
75. § 45-16.
76. http://europa.eu/rapid/press-release_IP-18-3343_fr.htm.
77. *Ibid.*
78. https://www.cnil.fr/fr/declaration-commune-adoptee-par-le-G29.
79. Avis de la CNCDH sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, 25 septembre 2014.
80. B. Oppetit, *Philosophie du droit*, Dalloz 1999, spéc. p 102.
81. Le Paquet *E-evidence* contient deux mesures complémentaires : une proposition Directive relative à la désignation d'un représentant légal dans l'Union assurant l'exécution des décisions et injonctions émises par les autorités compétentes des États membres et une proposition de règlement créant des injonctions européennes de production et de conservation des preuves électroniques.

ce point de vue, « *la conjonction des unilatéralismes* »[82] est évidente. Quel en sera le résultat ?

On se souvient que la Cour de Justice de l'Union européenne (CJUE)[83] avait invalidé purement et simplement la directive sur la conservation des données[84] et affirmé : « *cette directive engendrait une "ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soir limitée au strict nécessaire"* »[85]. La Cour avait également souligné : « *la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante*[86] ».

On peut craindre que les ingérences dénoncées dans cette décision ne se multiplient au nom d'impératifs sécuritaires largement compris, au risque de voir émerger des « démocratures »[87] au sein desquelles la sécurité se paiera du prix des libertés individuelles. ■

82. L. d'Avout, « Sanctions négociées, la nouvelle discipline étatique des entreprises mondiales », *Droits* n° 64, 2017.

83. CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.al.*, affaires jointes C-293/12 & C-594/12. Chron. M. Aubert, E. Broussy et H. Cassagnabère, D. 2014, 1355, note C. Castets-Renard, *ibid.* 2317, obs. J. Larrieu, C. C. le Stanc et P. Tréfigny.

84. Directive 2006/24.

85. *Ibid.*, § 65.

86. *Ibid.*, § 37.

87. Néologisme composé par le sociologue Gérard Mermet dans son livre *Démocrature : comment les médias transforment la démocratie*, Aubier, 1987.