Du *CLOUD Act* au règlement *E-evidence* La souveraineté à l'épreuve de l'accès aux données

par Marc Watin-Augouard
Général d'armée (2S) de la Gendarmerie nationale
Directeur du CREOGN
Fondateur du Forum International de la Cybersécurité (FIC)

Depuis l'affaire PRISM, révélée en 2013 par Edward Snowden, les données sont au cœur de relations conflictuelles entre l'Europe et les États-Unis. Il en est ainsi tout particulièrement des données à caractère personnel qui ne font pas l'objet d'un traitement similaire de part et d'autre de l'Atlantique. En effet, *privacy* et *« vie privée »* ne sont pas synonymes. L'annulation par la Cour de justice de l'Union européenne[1] du *Safe Harbor* et les critiques portant sur le *Privacy Shield*[2], sur fond de réactions outre-Atlantique à l'égard du règlement général relatif aux données à caractère personnel (RGPD), en sont des épisodes marquants.

S'agissant des données susceptibles de servir de preuves numériques, le *Warrant Case* Microsoft /*DoJ*, suivi de la publication du *CLOUD Act*, témoigne d'une volonté américaine de conférer à la loi une portée extraterritoriale, en contradiction avec la souveraineté des États et, par là-même, avec les règles qui président à la coopération internationale en matière judiciaire. Bien que la réflexion précède cette décision de l'administration Trump, le projet de règlement *E-evidence* apparaît comme une réponse de l'Union européenne au *CLOUD Act*.

Dans les deux cas, il s'agit de faciliter l'accès aux données numériques en réduisant les délais nécessaires à leur acquisition. Le *« temps de l'enquête »* est,

1. Arrêt CJUE C-362/14 *Maximillian Schrems/ Data Protection Commissionner,* 6 octobre 2015.
2. Résolution du Parlement européen du 5 juillet 2018 demandant à la Commission de suspendre le bouclier de protection des données jusqu'à ce que les autorités américaines se conforment aux dispositions de l'accord. L'examen annuel a eu lieu les 18 et 19 octobre 2018.

en effet, en décalage croissant avec l'accélération et la mobilité de la criminalité internationale, qu'elle vise le cyberespace ou qu'elle en exploite les possibilités. *E-evidence* est d'abord un instrument permettant d'améliorer les échanges entre les États membres. Mais le règlement n'est pas dépourvu, lui aussi, d'applications extraterritoriales. La confrontation pourrait entraîner un regain de tension, comme elle pourrait sous certaines conditions déboucher sur un accord transatlantique.

Dans ce contexte, une fois de plus, la souveraineté de la France est tributaire d'une souveraineté européenne, condition essentielle d'une troisième voie, alternative à la domination américaine ou chinoise.

I. *Warrant Case* Microsoft/*DoJ* au *CLOUD Act*, l'extraterritorialité de la loi américaine

Une bataille judiciaire, engagée aux États-Unis entre Microsoft et le Département de la Justice, aurait dû être stoppée par une décision de la Cour suprême américaine attendue en juin 2018. Cette querelle juridique n'était pas sans conséquence à l'encontre des données à caractère personnel des européens. Craignant sans doute un arbitrage contraire à ses volontés, Donald Trump a coupé court en promulguant, en mars, le *CLOUD Act*, en l'insérant sans véritable débat dans la loi de finances américaine.

A. Le *Warrant Case*

Par un arrêt du 14 juillet 2016, la Cour d'appel des États-Unis de la deuxième circonscription de New York[3] a annulé un jugement du tribunal fédéral de New York qui validait un mandat délivré par le Gouvernement des États-Unis contre Microsoft, en vertu de l'article 2 703 de la loi de 1986 sur les communications stockées *SCA* (*Stored Communications Act*[4]). Cette loi subordonne au Quatrième amendement[5] à la Constitution des États-Unis la communication par des fournisseurs de services de données exigées dans le cadre d'enquêtes judiciaires.

Par ce mandat émis en décembre 2013, le gouvernement américain exigeait de Microsoft la production d'un compte *e-mail* d'un client non-américain, utilisant

3. *Ruling of the US Court of Appeals for the 2nd Circuit of New York of 14 July 2016*.
4. Le *Stored Communications Act* est le chapitre 121 du Titre 18 du *United States Code* qui correspond au code pénal et au code de procédure pénale.
5. Cet amendement dispose que *« Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir »*.

les services de communications électroniques de l'entreprise et suspecté de trafic de stupéfiants. Pour satisfaire à cette requête, Microsoft aurait dû importer aux États-Unis des données stockées dans un *datacenter* situé en Irlande, données correspondant à des contenus. Pour Microsoft, une telle demande n'était pas légale. Pour respecter la souveraineté de l'Irlande, la demande aurait dû, selon Microsoft, suivre la procédure d'entraide judiciaire (*Mutual Legal Assistance Treaty – MLAT* ou commission rogatoire internationale) et donc passer par un juge.

Le cas d'espèce débouche sur un différend relatif à l'interprétation de la volonté du législateur. Lors de la promulgation du *SCA*, l'hypothèse d'un stockage des données localisées hors du territoire américain n'était pas envisagée, le *cloud* lui étant bien évidemment postérieur. Peut-on alors appliquer une loi à une situation non prévue par le Parlement américain ? La Cour d'appel a donné raison à Microsoft en tenant compte de l'intention première du législateur. Faute de preuve du contraire, les demandes gouvernementales en matière de transmission de données ne peuvent dépasser les frontières.

Le *Department of Jutice* (*DoJ*) s'est alors tourné vers la Cour suprême qui s'est saisie du dossier, en octobre 2017, et devait rendre sa décision en juin 2018. Il ne s'agissait pas dans le cas d'espèce d'une demande de données de connexion (adresse IP par exemple) qui peuvent être obtenues selon la procédure de la Convention de Budapest (art 18.1.b). Les États-Unis l'ont ratifiée (2007) mais pas l'Irlande…Il ne s'agissait pas non plus d'une demande effectuée dans le cadre d'un accord d'assistance judiciaire mutuel, mais d'une intrusion dans le *cloud*, hors des États-Unis, au seul prétexte que l'entreprise qui détient les données est une entreprise américaine.

La contestation de l'extraterritorialité est éludée par les autorités américaines qui appuient leur raisonnement sur l'accessibilité des données depuis les États-Unis. Peu importe, selon elles, le lieu de leur stockage qui peut varier selon des règles d'optimisation propres à l'hébergeur et compliquer les demandes d'entraide (à quel pays s'adresser ?). Le critère de l'accessibilité qu'elles opposent interdit toute manœuvre consistant dans le choix d'un pays non coopérant pour stocker des données en toute *« impunité »*. Par ailleurs, pour le *DoJ*, les données pouvant connaître des mouvements réguliers, de *datacenter* en *datacenter*, leur accès n'est opéré que sur le territoire américain, le transfert étant *« neutre »* au regard de la vie privée. Il ne s'agit donc pas d'une application de la loi hors des frontières mais d'une mesure relevant de la sécurité nationale, s'appliquant sur le territoire national.

Si l'on accepte la thèse gouvernementale, c'est toute l'architecture européenne qui veille à la protection et au transfert des données à caractère personnel qui est ébranlée. Par application du RGDP, Microsoft pourrait être condamné à une sanction pouvant atteindre 4 % de son chiffre d'affaire mondial. Le RGPD, dans son *« considérant »* 105, est très clair : *« Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à réglementer directement les*

activités de traitement effectuées par des personnes physiques et morales qui relèvent de la compétence des États membres. Il peut s'agir de décisions de juridictions ou d'autorités administratives de pays tiers qui exigent d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, et qui ne sont pas fondées 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. L'application extraterritoriale de ces lois, règlements et autres actes juridiques 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. Ce peut être le cas, entre autres, lorsque la divulgation est 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 ».

D'une manière générale, avec une extraterritorialité reconnue à la loi américaine, c'est l'équilibre des relations entre les États qui serait remis en cause, telle dictature exigeant par mimétisme l'obtention de données d'un opposant stockées sur le territoire d'une démocratie. Quelle serait par ailleurs l'utilité des accords bilatéraux dès lors qu'ils sont contournables ? Une telle décision accentuerait la *« balkanisation »* du cyberespace avec un stockage des données restreint à l'espace européen, voire aux territoires nationaux. Des solutions techniques empêchant l'accès aux données (chiffrement systématique avec clef conservée par le possesseur des données), des "*data trustees*[6]", intermédiaires non sollicitables puisque nationaux, pourraient faire écran et donc obstacle à l'accessibilité depuis les États-Unis (ou tout États tiers). Mais quel recul par rapport à une conception ouverte d'internet !

B. Le *CLOUD Act*

Le 23 mars 2018, Donald Trump ratifie le *CLOUD Act* (*Claryfing Lawful Overseas Use of Data*), *« glissé »* sans débat parmi les 2 232 pages de la loi de finances américaine. Est-ce par crainte d'une décision de la Cour suprême qui ne serait pas conforme à ses attentes ? Le *« cavalier législatif »* est trop important pour passer inaperçu. Il donne un cadre légal à la saisie de données par les autorités américaines lorsque celles-ci sont stockées hors des États-Unis. Il impose à toute entreprise relevant du droit américain de communiquer aux autorités américaines les données qu'elle détient, indépendamment du lieu où elles sont stockées.

Ces données doivent être liées à une enquête criminelle et concerner une personne ou un élément identifiant un particulier ; elles ne peuvent servir ensuite à une autre enquête. Selon le texte, *« un fournisseur de service de communication électronique ou de service informatique distant doit se conformer aux obligations du*

6. Exemple de Microsoft qui sous-traite ses *datacenter* à, T-Systems, en Allemagne.

présent chapitre pour préserver, sauvegarder ou divulguer le contenu d'un fil ou d'une communication électronique et 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 ». Le recours aux dispositions d'un *MLAT* (*Mutual Legal Assistance Treaty*) n'est plus nécessaire.

Le *CLOUD Act* consacre donc une forme d'extraterritorialité de la loi américaine contestée par Microsoft dans son litige avec le *DoJ* à propos de l'interprétation du *Stored Communications Act* de 1986. Même s'il s'applique à des sociétés américaines (les GAFAM en premier lieu), dont le siège est situé sur le territoire américain, l'impact s'observe hors des frontières US. Le fournisseur de service ne peut donc plus s'opposer, comme la société de Richmond l'a fait, à la remise de données stockées à l'étranger. Pour autant, le *CLOUD Act* lui ouvre des possibilités de recours, mais il lui appartient de se justifier, ce qui n'est guère confortable. Une possibilité lui est offerte dans le cas où le pays tiers a conclu un *executive agreement* avec les USA : un droit d'opposition (*comity analysis*) à déposer dans les quatorze jours après la notification, une requête en modification ou en annulation s'il croit *« raisonnablement »* que le client ou l'abonné n'est pas un citoyen des États-Unis et ne réside pas aux États-Unis et que la divulgation exigée créé un risque important de viol des lois d'un pays étranger.

Le juge américain examine le risque de sanction auquel est exposé le fournisseur dans l'autre pays et l'intérêt qui s'attache, pour la justice, à la modification ou à l'annulation de la demande. À défaut d'*executive agreement*, le fournisseur de service peut invoquer les *common law principles of comity*, principes de courtoisie internationale reconnus par les juridictions américaines qui les invitent à appliquer le droit américain à l'aune des intérêts du pays tiers. Cela rejoint la position de l'UE exprimée auprès de la Cour suprême : *« Selon l'Union européenne, du point de vue du droit international public, lorsqu'une autorité publique demande à une société établie dans sa propre juridiction de produire des données électroniques stockées sur un serveur situé dans une juridiction étrangère, les principes de territorialité et de courtoisie en droit international public sont engagés, et les intérêts et les lois de cette juridiction étrangère doivent être pris en compte »*.

Le *CLOUD Act* permet aussi aux pays étrangers, ayant passé avec les États-Unis un *executive agreement*, d'exiger des données personnelles stockées aux États-Unis, sans examen préalable par un juge, dès lors qu'il s'agit de lutter contre un *serious crime*. Mais ceci ne concerne pas les données des personnes physiques ou morales relevant du droit américain. L'*American Civil Liberties Union (ACLU)* a aussitôt critiqué le texte : *« Certaines entreprises technologiques (américaines) suggèrent que le* CLOUD Act *représente un progrès notable pour la protection des droits des consommateurs. Nous ne sommes pas d'accord. Nous pensons que le* Cloud Act *sape la vie privée et les autres droits de l'homme, ainsi que d'importantes garanties démocratiques »*.

II. *E-evidence*, la réponse européenne ?

L'Union européenne peut être inquiète, car ce texte semble contraire aux articles 44 et suivants du RGPD, relatifs aux *« Transferts ou divulgations non autorisés par le droit de l'Union »*. L'article 48 est particulièrement explicite : *« 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 »*. La demande s'appuyant sur le *CLOUD Act* peut aussi aller à l'encontre des dispositions de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016[7].

Le *CLOUD Act* a pour objectif de réduire le temps nécessaire à l'obtention des preuves numériques stockées hors des frontières. Est-ce un *« caprice américain »* ? La question de l'accès aux données dans le *cloud* est également au cœur des réflexions conduites par le Conseil de l'Europe dans le cadre de l'adaptation de la Convention de Budapest sur la cybercriminalité. C'est la même motivation qui soutient le projet de règlement *E-evidence*, même si la comparaison n'aboutit pas à une similitude. Il serait erroné d'affirmer que *E-evidence* est une réponse *« du berger à la bergère »*, car ses racines sont antérieures.

A. Un projet mûri depuis 2016

Le corpus juridique actuel de l'UE comprend notamment la directive 2014/41 / UE relative à la décision d'enquête européenne en matière pénale (directive EIO) qui doit établir un régime juridique unique pour l'obtention de preuves. Ces preuves contiennent bien sûr les données de souscription (Nom, prénom, date et lieu de naissance du titulaire d'un abonnement, adresse, etc.), les données de connexion ou métadonnées (heure et durée des appels, numéros des correspondants, coordonnées spatiales), et les données de contenu (courriels, mails, sms, fichiers, vidéos, photos). Mais cette directive suppose une transposition dans les droits nationaux qui peut faire apparaître des disparités. D'où l'idée d'un règlement immédiatement applicable au sein de l'Union.

7. Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. Cette directive a été transposée par le titre III de la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

À la suite des attentats terroristes qui ont endeuillé Bruxelles, le 22 mars 2016, les ministres européens de la Justice et des Affaires intérieures sont convenus qu'il fallait, en priorité, adopter des mesures visant à rendre la collecte et l'obtention de preuves numériques plus efficiente et plus efficace. Lors de la session du Conseil de l'Union européenne (justice et affaires intérieures), tenue à Luxembourg les 9 et 10 juin 2016, le Conseil a appelé à une action concrète fondée sur une approche commune de l'UE pour rendre l'entraide judiciaire plus efficace dans le cyberespace.

Le 17 avril 2018, la Commission a proposé dans une communication (COM (2018) 225 final) de nouvelles dispositions[8] permettant aux autorités judiciaires et aux services enquêteurs d'obtenir plus rapidement les preuves numériques stockées dans le cloud. Article 82 (1) *provides that measures may be adopted in accordance with the ordinary legislative procedure to lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions*. Pour Frans Timmermans, premier vice-président de la Commission : *« Les preuves électroniques revêtent une importance croissante en matière pénale. Nous ne pouvons pas accepter que les criminels et les terroristes exploitent les technologies de communication électroniques modernes pour dissimuler leurs actes et se soustraire à la justice. Les criminels et les terroristes ne doivent pouvoir trouver aucun refuge en Europe, que ce soit en ligne ou hors ligne. Les propositions présentées aujourd'hui visent non seulement à mettre en place de 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 les libertés de toutes les personnes concernées »*.

Věra Jourová, commissaire européen en charge de la Justice, souligne l'inégalité qui s'établit entre les criminels et la justice : *« Alors que les autorités répressives continuent de 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 »*. La Commission constate que pour près de deux tiers des infractions, les preuves électroniques sont détenues dans un autre pays ; les enquêtes ou les poursuites ne peuvent pas être menées correctement, principalement en raison du délai nécessaire pour recueillir ces preuves ou à cause de la fragmentation du cadre juridique.

B. Un règlement en cohérence avec la Convention de Budapest

Comme le souhaite la Commission, les autorités des États membres doivent avoir accès aux données qui pourraient servir de preuve et qui sont stockées

8. *Proposal for a regulation of the European parliament and of the council on European Production and Preservation Orders for electronic evidence in criminal matter.*

en dehors de leur pays et/ou par les prestataires de services dans d'autres États membres ou dans des pays tiers. Le règlement a donc une portée extraterritoriale hors de l'UE. Le projet de règlement prévoit deux injonctions : une injonction de production de données et une injonction de conservation de données. Ces injonctions s'appuient sur le principe de reconnaissance mutuelle : l'intervention d'une autorité judiciaire d'un États *« cible »* n'étant pas requise, dès lors qu'elle émane d'un juge de l'États *« source »*.

L'article 82, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne (TFUE) prévoit, en effet, que des mesures peuvent être prises conformément à la procédure législative ordinaire, pour établir des règles et de procédures visant à assurer la reconnaissance dans toute l'Union de toutes les formes de jugements et de décisions judiciaires. Dans les deux cas, l'infraction doit avoir été déjà commise, que l'auteur soit connu ou inconnu. Contrairement au *CLOUD Act*, les procédures d'injonctions sont strictement encadrées par les autorités judiciaires.

La Convention de Budapest sur la cybercriminalité (STCE n° 185) du 23 novembre 2001 du Conseil de l'Europe prévoit des mécanismes internationaux de coopération contre la cybercriminalité. Elle invite les parties à mettre en œuvre des procédures permettant d'obtenir des preuves électroniques et de se prêter mutuellement assistance juridique, sans se limiter aux infractions propres au cyberespace. La Convention exige des parties qu'elles mettent en place des ordres de production pour obtenir des données informatiques auprès des fournisseurs de services sur leur territoire et des données sur les abonnés auprès des fournisseurs de services offrant des services sur leur territoire. En outre, la Convention prévoit des ordonnances de conservation lorsqu'il existe des raisons de croire que les données informatiques sont particulièrement vulnérables à la perte ou à la modification. Dans les deux cas, il s'agit d'actes d'enquête. Les offreurs de services sont les fournisseurs de services de communication électronique, les fournisseurs de services de la société de l'information pour lesquels le stockage des données est un élément déterminant du service fourni à l'utilisateur (y compris les réseaux sociaux qui ne sont pas des services de communications électroniques), les places de marchés en ligne facilitant les transactions entre leurs utilisateurs (tels que les consommateurs ou les entreprises), les fournisseurs de services d'hébergement et fournisseurs d'infrastructure Internet tels que les adresses IP et les registres de noms de domaine.

C. Les injonctions de production et de conservation

Le projet de règlement *E-evidence* s'inscrit bien dans la cadre de la Convention. Il envisage tout d'abord de créer une injonction européenne de production de données. Cette procédure doit permettre à une autorité judiciaire d'un État membre de demander des preuves électroniques (courriels, SMS, messages échangés dans des applications) directement auprès d'un offreur de services dans l'Union

et établi ou représenté dans un autre État membre et ce, indépendamment de la localisation des données. L'offreur de services est alors tenu de répondre dans un délai de 10 jours, et dans les 6 heures en cas d'urgence (actuellement 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire). L'injonction de production de données de connexion (abonnés ou accès) peut être délivrée pour toute infraction pénale. En revanche les données transactionnelles ou de contenu ne peuvent être délivrée que pour des infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'au moins trois ans. Il en est de même pour certaines infractions visées par le règlement[9]. Cette différence se justifie par le caractère nettement plus intrusif des investigations nécessaires.

Une seconde mesure veut empêcher l'effacement de données par le biais d'une injonction européenne de conservation, une sorte de *« gel numérique »*. L'autorité judiciaire d'un État membre peut, après une évaluation individuelle de la proportionnalité et de la nécessité, contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données, afin que cette autorité puisse obtenir ces informations ultérieurement, par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production. L'ordre de préservation européen ne permet que la conservation des données déjà stockées au moment de la réception de la demande. Le champ du règlement ne couvre donc par les interceptions en temps réel.

Ces deux procédures s'accompagnent de garanties et de voies de recours : les deux injonctions sont produites dans le cadre de procédures pénales et bénéficient donc des garanties procédurales de droit pénal. Un juge judiciaire contrôle *ex-ante*, soit parce qu'il est lui-même à l'origine de la demande, soit parce qu'il autorise une initiative venant du parquet ou des services enquêteurs. C'est sans doute une des principales différences avec le *CLOUD Act* qui n'exige pas l'intervention d'un juge.

---

9. Ces infractions sont des dispositions spécifiques de la décision-cadre 2001/413/JAI du Conseil relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, la pornographie enfantine et remplaçant la décision-cadre 2004/68 / JAI du Conseil et la directive 2013/40 / UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222 / JAI du Conseil. *Orders may also be issued for offences listed in Directive 2017/541/EU on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*. Des ordonnances peuvent également être prises pour des infractions énumérées dans la directive 2017/541 / UE relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475 / JAI du Conseil et modifiant la décision 2005/671 / JAI du Conseil. *Some of these offences have minimum maximum thresholds of at least 1 year, others of 2 years, but none goes below a maximum threshold of 1 year*. Certaines de ces infractions ont des seuils minimaux d'au moins 1 an, d'autres de 2 ans, mais aucun ne se situe au-dessous d'un seuil maximum de 1 an.

Les offreurs de services et les personnes dont les données sont demandées bénéficieront de plusieurs garanties pour assurer la protection des droits individuels et de la courtoisie internationale. Parmi ces garanties, la possibilité, pour le prestataire de services, de demander un réexamen si, par exemple, l'injonction constitue une violation manifeste de la Charte des droits fondamentaux de l'Union européenne. C'est le cas également en cas de conflit de lois, lorsque des prestataires de services ayant leur siège dans des pays tiers sont confrontés à des obligations contradictoires. Comme le précisent les articles 15 et 16 du projet de règlement : *« Si le tribunal détermine qu'il existe effectivement un conflit d'obligations découlant des lois protégeant les droits fondamentaux des personnes ou des intérêts fondamentaux du pays tiers en matière de sécurité nationale ou de défense, le tribunal doit demander l'avis du pays tiers concerné via les autorités du pays tiers. Si le pays tiers consulté confirme l'existence du conflit et s'oppose à l'exécution de l'ordonnance, le tribunal doit retirer l'ordonnance »*.

Ces dispositions, en fixant des normes élevées, encouragent les pays tiers à assurer un niveau de protection similaire. Dans le cas inverse, lorsque les autorités d'un pays tiers cherchent à obtenir des citoyens européens un fournisseur de services de l'UE, les lois de l'Union ou des États membres protégeant les droits fondamentaux, comme l'acquis en matière de protection des données, peuvent également empêcher la divulgation. L'Union européenne attend des pays tiers qu'ils respectent ces interdictions, allusion à peine cachée au *CLOUD Act*. Quant aux personnes suspectées, elles doivent bénéficier d'une possibilité de recours devant une juridiction de l'État d'émission pour contester la légalité, la nécessité ou la proportionnalité de l'injonction, disposition qui n'est pas exclusive d'un recours exercé au titre de la directive 2016/680 ou du RGPD.

Les offreurs de service doivent désigner un représentant légal dans l'Union, même si leur siège est situé dans un pays tiers, pour la réception, le respect et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres à des fins de collecte de preuves en matière pénale. Le règlement sera également applicable si les prestataires de services ne sont pas établis ou représentés dans l'Union, mais y offrent des services.

Le projet de règlement doit, désormais, entrer dans la procédure du trilogue (Conseil, Commission, Parlement) après la prise de position favorable du Conseil, le 7 décembre 2018. À cette occasion, Josef Moser, ministre autrichien de la Justice, a rappelé que *« les preuves numériques deviennent un élément crucial des procédures pénales. Aujourd'hui, les délinquants recourent à des technologies de pointe rapides qui ne s'arrêtent pas aux frontières. Ces nouvelles règles remplaceront les actuelles méthodes complexes par des moyens rapides et efficaces de collecter et d'échanger des preuves numériques par-delà les frontières. Cette évolution contribuera à la protection de nos citoyens, et ce sans mettre en péril leurs droits et leurs libertés »*.

La promulgation du règlement ne pourra intervenir avant le renouvellement du Parlement, en mai 2019. S'il était approuvé par le futur parlement, il n'entrerait en vigueur au plus tôt en 2021, voire 2022…Au-delà se pose la question des

relations transatlantiques. L'accélération de l'obtention des preuves numériques est une nécessité partagée des deux côtés. Peut-on imaginer un *« cessez-le-feu »*, voire un accord entre les Européens et les Américains, même si ces derniers ne semblent pas envisager d'accord avec l'UE en privilégiant des *Gentlemen agreements* d'États à États. Comme le souligne Théodore Christakis[10], *« le* CLOUD Act *ne prévoit la possibilité de conclure des accords qu'avec des "gouvernements", pas avec des organisations internationales telles que l'Union européenne »*. C'est pourtant ce que souhaite la Commission européenne. Le 5 février 2019, faisant suite aux conclusions du Conseil européen d'octobre 2018, elle adresse une recommandation au Conseil *« autorisant l'ouverture de négociations en vue d'un agrément entre l'Union européenne et les États-Unis sur l'accès transfrontalier à la preuve numérique pour une coopération judiciaire contre la criminalité »*. L'établissement d'une entente cordiale transatlantique est nécessaire !

10. www.observatoire-fic.com, 28 juin 2018.