Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

E-Avis ISDC 2018-05

L'ACCES AUX CONTENUS DE MESSAGERIES ELECTRONIQUES ET RESEAUX SOCIAUX STOCKES A L'ETRANGER DANS LE CADRE D'ENQUETES PENALES

Droits de l'Union européenne et du Conseil de l'Europe, Allemagne, Autriche, Belgique, Etats-Unis, France, Irlande, Italie

Etat au : 01.03.2018

Citation suggérée : C. Viennet, I. Blatter, J. Curran, K.T. Druckman, J. Fournier, A.-C. Pierrat, I. Pretelli, S. Tscheulin, L'accès aux contenus de messageries électroniques et réseaux sociaux stockés à l'étranger dans le cadre d'enquêtes pénales, état au 01.03.2018,
E-Avis ISDC 2018-05, disponible sur www.isdc.ch.

E-Avis ISDC
Série de publications électroniques d'avis de droit de l'ISDC / Elektronische Publikationsreihe von Gutachten des SIR / Serie di pubblicazioni elettroniche di pareri dell'Istituto svizzero di diritto comparato / Series of Electronic Publications of Legal Opinions of the SICL

TABLE DES MATIERES

I. FAITS

L'Office fédéral de la Justice a mandaté l'Institut suisse de droit comparé pour la rédaction d'un avis de droit concernant l'accès par des autorités de poursuite pénale à des données contenues dans des réseaux sociaux et courriers électroniques et stockées à l'étranger. Les juridictions dont l'étude a été demandées sont celles de l'Allemagne, l'Autriche, la Belgique, les Etats-Unis, la France, l'Irlande et l'Italie.

Cette demande s'inscrit dans le cadre du dépôt d'une motion visant à « faciliter l'accès des autorités de poursuite pénale aux données des réseaux sociaux »[1], en obligeant les réseaux sociaux « proposant des services destinés aux consommateurs suisses et traitant des données personnelles à ces fins [à] dispose[r] d'une représentation en Suisse qui [ait] le pouvoir de transmettre directement aux autorités de poursuite pénale suisses les données nécessaires à une procédure pénale, sans que ces dernières n'aient à passer par l'entraide pénale internationale »[2]. Cette motion a été déposée suite à un arrêt du Tribunal fédéral du 16 novembre 2016 décidant que, en vertu du droit actuellement en vigueur, le ministère public ne peut exiger des données personnelles d'utilisateurs impliqués dans une procédure pénale auprès de Facebook Suisse, ce dernier n'étant pas titulaire des données et n'étant pas lié à la société irlandaise qui les détient, et que le ministère public « n'a dès lors d'autre choix que de s'adresser aux autorités irlandaises pour obtenir les renseignements désirés »[3].

II. QUESTIONS

Les questions posées par l'Office fédéral de la justice à l'Institut sont les suivantes :

1. Comment les autorités de poursuite pénale peuvent avoir accès à des données stockées à l'étranger dans des messageries électroniques et sur des réseaux sociaux : par entraide judiciaire internationale en matière pénale ? Est-ce qu'il y a des possibilités d'accès direct (par les comptes d'utilisateurs, des établissements du « Host », des plateformes ou autres) ?

   Si un accès direct est possible, en vertu de quelle norme ? Y a-t-il de la jurisprudence ?
2. Des réformes concernant l'accès des autorités de poursuite pénale à des données à l'étranger contenues dans des messageries électroniques et des réseaux sociaux sont-elles prévues ?
3. Une autorité de poursuite pénale étrangère se rend-elle coupable d'une infraction si elle accède directement aux données contenues dans des messageries électroniques et des réseaux sociaux sur le territoire de l'Etat ?

III. ANALYSE

A. UNION EUROPÉENNE ET CONSEIL DE L'EUROPE

1. Droit en vigueur

La question de **l'entraide judiciaire internationale est touchée**, dans le domaine du présent avis, **au niveau européen par deux principaux instruments** : la Convention sur la cybercriminalité du Conseil

---

1 Motion déposée par C. Levrat, Faciliter l'accès des autorités de poursuite pénale aux données des réseaux sociaux, déposée au Conseil d'Etat le 15.12.2016.

2 Présentation du texte déposé, disponible sous : https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164082 (15.12.2017).

3 Arrêt du Tribunal fédéral, 16.11.2016, 143 IV 21, N 3.4.3.

de l'Europe[4], et la Directive concernant la décision d'enquête européenne en matière pénale pour les Etats membres de l'Union européenne[5].

La **Convention sur la cybercriminalité du Conseil de l'Europe**, ouverte à la signature dès 2001, est le premier accord international sur les infractions pénales commises par le biais de l'internet et des réseaux informatiques et comprend notamment les mesures procédurales à adopter pour les perquisitions et saisies de données à l'étranger, ainsi que des règles visant à l'amélioration de la coopération internationale.[6] A l'heure actuelle, cette convention a été ratifiée par 43 des 46 Etats membres du Conseil de l'Europe dont l'Allemagne, l'Autriche, la Belgique, la France et l'Italie. Toutefois, cet instrument ne concerne pas seulement le niveau européen puisque 13 pays d'autres continents l'ont également ratifié, tels que les Etats-Unis, le Japon et l'Australie.[7] La Convention sur la cybercriminalité est ainsi le principal instrument international en matière d'accès aux données stockées à l'étranger dans le cadre d'enquêtes pénales.

Au niveau de l'Union européenne, **la Directive 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne** remplace les mécanismes d'entraide judiciaire existants, principalement la Convention relative à l'entraide judiciaire de l'UE de 2000[8] et la Décision-cadre relative au mandat européen d'obtention de preuves de 2008[9]. 21 des 28 Etats membres de l'Union européenne ont pris des mesures de transposition de la Directive. Deux Etats, l'Irlande et le Danemark, ne participent pas à son adoption. Cette directive vise à améliorer les enquêtes criminelles transfrontalières au sein de l'Union européenne en instaurant la décision d'enquête européenne qui concerne l'obtention de preuves entre pays. La décision d'enquête européenne est émise ou validée par une autorité judiciaire d'un Etat membre et impose à celle d'un autre Etat membre d'exécuter, dans les plus brefs délais, la demande d'obtention ou de transmission d'éléments de preuves (sauf possibilités de refus limitées). Contrairement à la Convention sur la cybercriminalité, la Directive s'étend à la récupération d'éléments de preuve dans le cadre d'infractions pénales en général, et pas seulement de « cyber-infractions ».

---

4 Convention sur la cybercriminalité, ouverte à la signature le 23.11.2001, entrée en vigueur le 01.07.2004, disponible sous : https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/090000168008156d (22.12.2017).

5 Directive 2014/41/UE du Parlement européen et du Conseil du 03.04.2014 concernant la décision d'enquête européenne en matière pénale, délai de transposition dans les Etats membres au 22.05.2017, disponible sous : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014L0041 (22.12.2017).

6 L. Meyer-Gossner & B. Schmitt, Beck'scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, vor § 94, Rn. 10.

7 Etat des signatures et ratification de la Convention sur la cybercriminalité disponible sous : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_aut=snFociTl (22.12.2017).

8 Convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, établie par acte du Conseil du 29.05.2000, disponible sous : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000F0712(02)&from=FR (22.12.2017).

9 Décision-cadre 2008/978/JAI du Conseil du 18.02.2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales (plus en vigueur), disponible sous : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32008F0978 (22.12.2017).

2. Réformes prévues

En juin 2016, le Conseil de l'Union européenne a adopté des conclusions pour l'amélioration de la justice pénale dans le cyberespace[10] relatives à la rationalisation des procédures d'entraide judiciaire et l'amélioration de la coopération avec les fournisseurs de service[11]. Ainsi, le Conseil demande à la Commission européenne, en association avec les Etats membres, d'explorer, avec les fournisseurs de service, les possibilités pour établir un cadre et des outils communs pour faciliter et renforcer les procédures visant à l'obtention des preuves électroniques[12] ; la Commission est encore chargée d'explorer les différentes solutions possibles pour les situations dans lesquelles les normes existantes ne sont pas suffisantes, par exemple lorsque les preuves électroniques changent de juridiction en un très court instant[13] (cf. à ce sujet également les propositions de l'Allemagne, mentionnées sous B., 2.).

Ainsi la Commission a déployé une série d'efforts. En particulier, elle a régulièrement produit des « rapports sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective » [14]. Elle prévoit de mettre en place des « mesures concrètes visant à améliorer l'accès transfrontière aux preuves électroniques dans les enquêtes pénales, notamment en finançant la formation en matière de coopération transfrontière, en élaborant une plateforme électronique pour l'échange d'informations au sein de l'UE et en standardisant les formes de coopération judiciaire utilisées entre les Etats membres »[15]. Dans ce cadre, **la Commission a lancé un processus de consultation** d'experts, qui a donné lieu à l'identification de mesures pratiques et législatives indiquées pour améliorer l'accès transfrontalier aux preuves électroniques[16], ainsi qu'une consultation

---

10 Conseil de l'UE, Council conclusions on improving criminal justice in cyberspace, 09.06.2016, disponible sous : http://www.consilium.europa.eu/media/24300/cyberspace-en.pdf (22.12.2017); Conseil de l'UE, Council conclusions on the European judicial cybercrime network, 09.06.2016, disponible sous : http://www.consilium.europa.eu/media/24301/network-en.pdf (22.12.2017).

11 Voir notamment : Communiqué de presse : Lutte contre les activités criminelles dans le cyberespace : le Conseil convient de mesures pratiques et des prochaines étapes, 09.06.2016, disponible sous : http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09/criminal-activities-cyberspace/ (22.12.2017).

12 Conseil de l'UE, Council conclusions on improving criminal justice in cyberspace, 09.06.2016, *op. cit.*, N I § 3.

13 Conseil de l'UE, Council conclusions on improving criminal justice in cyberspace, 09.06.2016, *op. cit.*, N III § 10.

14 Voir notamment : Commission européenne, Rapport de la Commission au Parlement européen, au Conseil européen et au Conseil. Sixième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, 12.04.2017, COM(2017) 213 final, pp. 7 – 8, disponible sous : https://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-213-F1-FR-MAIN-PART-1.PDF (06.02.2018) ; Commission européenne, Communication de la Commission au Parlement européen, au Conseil européen et au Conseil. Huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, 29.06.2017, COM(2017) 354 final, p. 6, disponible sous : http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-354-F1-FR-MAIN-PART-1.PDF (06.02.2018).

15 Commission européenne, Communication conjointe au Parlement européen et au Conseil. Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide, 13.09.2017, JOIN(2017) 450 final, p. 17, disponible sous : http://data.consilium.europa.eu/doc/document/ST-12211-2017-INIT/fr/pdf (06.02.2018).

16 Services de la Commission européenne, Non-paper from the Commission services. Improving cross-border access to electronic evidence : Findings from the expert process and suggested way forward, disponible (en anglais) sous : https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (26.01.2018); Services de la Commission européenne, Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving criminal justice in cyberspace, disponible (en anglais) sous: https://ec.europa.eu/home-

publique[17] et la consultation des Etats membres sous la forme d'un questionnaire relatif aux pratiques nationales en matière de coopération directe entre les autorités de poursuite pénale et les fournisseurs de service du secteur privé, d'entraide judiciaire et d'autres mesures que les autorités utilisent pour obtenir des preuves lorsqu'il est incertain qu'elles agiront dans leur propre juridiction[18]. Enfin, **la Commission européenne envisage de proposer une directive pour améliorer l'accès transfrontière aux preuves électroniques en matière pénale** début 2018[19].[20] Pour sa part, le **Parlement européen** a adopté une résolution sur la lutte contre la criminalité le 3 octobre 2017[21], dans laquelle il insiste sur la nécessité de trouver des moyens de recueillir des preuves électroniques plus rapidement et de manière licite, ainsi que sur l'importance d'une coopération étroite entre les autorités répressives, les pays tiers et les fournisseurs de services actifs sur le territoire européen. Le Parlement indique que la Commission devrait proposer un cadre juridique européen pour les preuves électroniques offrant, d'une part, les garanties suffisantes concernant les droits et les libertés de toutes les parties concernées et comprenant, d'autre part, des règles harmonisées pour déterminer le statut des fournisseurs de services, national ou étranger, et obliger ces derniers à répondre aux demandes en provenance d'autres Etats membres[22].

En parallèle, l'usage par des autorités nationales du **piratage informatique** pour accéder à des données privées a conduit l'Union européenne à envisager l'adoption de mesures dans ce domaine[23]. L'une des problématiques soulevées tient au respect de la souveraineté territoriale lorsque la localisation géographique des données est inconnue[24].

Im **Europarat** hat das **Comité de la Convention Cybercriminalité (T-CY)** im November 2011 eine „Groupe ad hoc du T-CY sur l'accès transfrontalier aux données et sur les questions de compétence

---

affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf (26.01.2018).

17 Commission européenne, Public consultation in improving cross-border access to electronic evidence in criminal matters, disponible sous : https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en#about-this-consultation (06.02.2018).

18 Réponses des Etats membres de l'UE au « Questionnaire for EU Member states following the 9 June 2016 Conclusions of the JHA on improving criminal justice in cyberspace », disponible (en anglais) sous : https://www.asktheeu.org/en/request/responses_to_the_questionnaire_o (06.02.2018); Questionnaire on improving criminal justice in cyberspace. Summary of responses, disponible (en anglais) sous : https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf (06.02.2018).

19 Commission européenne, Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide, *op. cit.*, p. 21 ; Commission européenne, Inception impact assessment, disponible (en anglais) sous : https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en (06.02.2018).

20 Commission européenne, E-evidence, disponible (en anglais) sous : https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (26.01.2018).

21 Résolution du Parlement européen du 03.10.2017 sur la lutte contre la cybercriminalité, disponible sous : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//FR (06.02.2018).

22 Résumé du texte adopté du Parlement, disponible sous : http://www.europarl.europa.eu/oeil/popups/summary.do?id=1506097&t=d&l=fr (06.02.2018).

23 Directorate-general for Internal policies, Legal frameworks for hacking by law enforcement : identification, evaluation and comparison of pratices. Study for the LIBE committee, 2017, pp. 69 – 71, disponible (en anglais) sur : http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (09.02.2018).

24 Directorate-general for Internal policies, Legal frameworks for hacking by law enforcement: identification, evaluation and comparison of pratices, *op. cit.*, p. 9 et pp. 27 – 30.

territoriale“ gegründet.[25] Diese Gruppe wurde unter anderem damit beauftragt, die Anwendung von Artikel 32 Buchstabe b) der Cybercrime-Konvention zu untersuchen und ein Instrument auszuarbeiten, um den grenzüberschreitenden Zugriff auf Daten besser zu regulieren.[26] Zudem wurde vom Comité de la Convention Cybercriminalité im Dezember 2014 die „Groupe de travail sur les preuves dans le cloud“[27] gegründet und damit beauftragt, Lösungen zu prüfen betreffend den Zugang von Strafverfolgungsbehörden zu in einer Cloud gespeicherten Beweismitteln, insbesondere im Rahmen der internationalen Rechtshilfe.[28]

B. ALLEMAGNE

1. Zugriff der Strafverfolgungsbehörden auf im Ausland gespeicherte Daten

1.1. Übersicht

In den deutschen Bundesgesetzen findet sich mit § 110 Absatz 3 Strafprozessordnung lediglich eine Rechtsgrundlage für den Zugriff auf im Inland gespeicherte elektronische Daten. Inwiefern diese Befugnis auf transnationales Cloud-Computing anwendbar ist, ist in der Literatur derzeit noch umstritten (s. dazu unten, 1.2.). Ein **grenzüberschreitender Fernzugriff** auf **im Ausland gespeicherte Daten** bedarf grundsätzlich eines **förmlichen Rechtshilfeersuchens**.[29]

Auf im Ausland gespeicherte elektronische Daten ist der Zugriff nur bedingt möglich, nämlich lediglich im Rahmen der Artikel 29 und 32 Cybercrime-Konvention sowie der Richtlinie über die Europäische Ermittlungsanordnung (s. dazu unten, 1.3.). Zudem erlaubt nach deutscher Auslegung das Gewohnheitsrecht in Einklang mit Artikel 32 Buchstabe a) der Cybercrime-Konvention Zugriff auf offen zugängliche Daten.

Eine **Direktanfrage** bei den ausländischen **Provider-Firmen** seitens der deutschen Strafverfolgungsbehörden scheint erlaubt zu sein. Allerdings besteht auf die Direktanfrage hin **kein Anspruch** auf Herausgabe, sie beruht auf Freiwilligkeit seitens der Provider.[30] Die Direktanfragen zwischen

---

25 Accès transfrontalier aux données et compétence : options concernant l’action future du T-CY, S. 4, verfügbar unter https://www.coe.int/fr/web/cybercrime/t-cy-reports (17.11.2017).

26 Groupe ad hoc du T-CY sur l’accès transfrontalier aux données et sur les questions de compétence territoriale : mandat, S. 3, verfügbar unter https://www.coe.int/fr/web/cybercrime/t-cy-reports (17.11.2017).

27 Informationen dazu sind verfügbar unter https://www.coe.int/fr/web/cybercrime/ceg (17.11.2017).

28 Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY, S. 4, verfügbar unter https://www.coe.int/fr/web/cybercrime/t-cy-reports (17.11.2017).

29 B. Gercke, in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 28; L. Meyer-Gossner & B. Schmitt, Beck’scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7a.

30 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Eva Bulling-Schröter, weiterer Abgeordneter und der Fraktion DIE LINKE, Bundestags-Drucksache 18/10948, S. 4, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/109/1810948.pdf (20.10.2017). In unserem Bericht wird nicht weiter darauf eingegangen, ob gemäss Art. 32 Buchst. b) Cybercrime-Konvention (CCC) neben dem Nutzer auch die Provider-Firma rechtmässig befugt ist, Daten an die Strafverfolgungsbehörden weiterzugeben, soweit die Provider-Firma dies in den Allgemeinen Nutzungsbedingungen vorgesehen hat. Ob dies dem Willen der Konventionsstaaten entspricht, lässt sich auch mithilfe des erläuternden Berichts der Cybercrime-Konvention (N 294), verfügbar unter https://www.coe.int/de/web/conventions/full-list/-_/conventions/treaty/185 (17.11.2017), nicht abschliessend klären. Allerdings scheint es gemäss dem Comité de la Convention Cybercriminalité (T-

Strafverfolgungsbehörden und sozialen Netzwerken werden durch das am 1. Oktober 2017 in Kraft getretene Netzwerkdurchsetzungsgesetz (NetzDG) erleichtert. Dieses Gesetz verpflichtet Anbieter von sozialen Netzwerken, *„[f]ür Auskunftsersuchen einer inländischen Strafverfolgungsbehörde […] eine empfangsberechtigte Person im Inland zu benennen*."[31] Ziel der Regelung ist es, sicherzustellen, dass die sozialen Netzwerke einen „Briefkasten" im Inland bereitstellen. Die Vorschrift gilt für alle sozialen Netzwerke unabhängig von ihrem Sitz im Inland oder im Ausland. Dadurch werden jedoch lediglich die Möglichkeiten einer freiwilligen unmittelbaren Kooperation zwischen Strafverfolgungsbehörden und Anbietern von sozialen Netzwerken verbessert, jedoch keine zusätzlichen Auskunftspflichten begründet.[32]

1.2. Zugriff auf Daten im Inland

Der Zugriff der Strafverfolgungsbehörden auf im **Inland** gespeicherte elektronische Daten ist durch **§ 110 Absatz 3 Strafprozessordnung (StPO)[33]** geregelt:

> *„(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend."*

§ 110 Absatz 3 Strafprozessordnung erlaubt als rein nationale Befugnisnorm einen Zugriff auf ein räumlich getrenntes Speichermedium nur, soweit sich dieses im **deutschen Hoheitsgebiet** befindet.[34] Voraussetzung ist, dass eine Erweiterung der Durchsicht auf andere über ein Netzwerk angeschlossene Speichermedien technisch möglich ist. Werden im Rahmen der Durchsuchung **Passwörter** für den Zugang zu solchen externen Speichermedien des Betroffenen gefunden, ist ein Abruf der dortigen Informationen ebenfalls zulässig.[35]
Speziell zu erwähnen sind die Daten beim transnationalen ***„Cloud-Computing"***[36], bei dem normalerweise nicht feststellbar ist, in welchem Hoheitsgebiet sich die Daten befinden. Die deutsche Rechtslehre ist diesbezüglich geteilter Meinung.[37] Für einen Teil der Lehre dürfte es sich um eine von Artikel 110 Absatz 3 Strafprozessordnung gedeckte, rechtmässige Ermittlungshandlung im Inland

---

CY) eher unwahrscheinlich, dass die Provider-Firma die Voraussetzungen der rechtmässigen und freiwilligen Zustimmung erfüllen (Accès transfrontalier aux données et compétence : options concernant l'action future du T-CY, S. 21, verfügbar unter https://www.coe.int/fr/web/cybercrime/t-cy-reports (17.11.2017)).

31 § 5 Abs. 2 S. 1 Netzwerkdurchsetzungsgesetz (NetzDG).

32 Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, Bundestags-Drucksache 18/12356, S. 27, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/123/1812356.pdf (20.10.2017).

33 Art. 110 Abs. 3 Strafprozessordnung (StPO) erlaubt nur die offene Durchsicht von Daten auf externen Speichermedien, nicht den heimlichen Zugriff auf Computersysteme im Sinne einer Online-Durchsuchung (M. Tsambikakis, in V. Erb *et al*. (Hrsg.), StPO Band 3, 26. Aufl., Berlin 2014, § 110, Rn. 8).

34 B. Gercke in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 26; L. Meyer-Gossner & B. Schmitt, Beck'scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 6.

35 W. Bär, Transnationaler Zugriff auf Computerdaten, Zeitschrift für Internationale Strafrechtsdogmatik 2011, S. 54; B. Gercke, in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 24; M. Tsambikakis in V. Erb *et al*. (Hrsg.), StPO Band 3, 26. Aufl., Berlin 2014, § 110, Rn. 8.

36 „Cloud-Computing" wird definiert als die Nutzung von IT-Infrastrukturen und -Dienstleistungen, die nicht vor Ort auf lokalen Rechnern gespeichert, sondern als Dienst gemietet werden und auf welche über ein Netzwerk (zum Beispiel das Internet) zugegriffen wird (vgl. Duden).

37 Es scheint noch keine Gerichtsentscheide zu dieser Problematik des Cloud-Computing zu geben.

handeln, soweit der Fernzugriff auf das externe Speichermedium vom Computer des betroffenen *Cloud*-Nutzers über dessen Account erfolgt.[38] Die Sichtung nach § 110 Absatz 3 Strafprozessordnung sei zulässig, wenn unklar sei, ob und in welchem ausländischen Staat sich der Server befinde, auf dem die Daten des Betroffenen gespeichert seien.[39] Der andere Teil der Lehre verlangt in jedem Fall ein Rechtshilfeersuchen gegenüber dem Staat des Serverstandortes.[40] Könne nicht zweifelsfrei ermittelt werden, ob sich die Daten in einem fremden Hoheitsgebiet befinden, so hätte ein Fernzugriff im Zweifel zu unterbleiben.[41] Nach Meinung der Bundesregierung ist ein Fernzugriff auf *Cloud*-Daten, wenn der physische Ort des Servers unbekannt ist, „von den zuständigen Strafverfolgungsbehörden nach Massgabe des jeweiligen Einzelfalls unter Berücksichtigung der nationalen Befugnisnormen und der anwendbaren völkerrechtlichen Verträge zu entscheiden.“[42]

Darüber hinaus gestattet das deutsche Recht nunmehr auch ausdrücklich die sogenannte „**Online-Durchsuchung**“ im Rahmen der **Strafverfolgung**. Während die Rechtsprechung die Befugnis hierzu zuvor lediglich aus einer Annex-Kompetenz herleitete,[43] ist die Online-Durchsuchung seit dem 24. August 2017 nun ausdrücklich in **§ 100b Strafprozessordnung** geregelt. Demnach darf „[a]uch ohne Wissen des Betroffenen […] mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung) […]“.[44]

Im Rahmen der **Gefahrenabwehr durch das Bundeskriminalamt gegen Gefahren des internationalen Terrorismus** ist eine solche **Online-Durchsuchung** bereits seit 2009 möglich. Dies ergibt sich derzeit[45]

---

38 L. Meyer-Gossner & B. Schmitt, Beck’scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7b; M. Wicker, Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, Multimedia und Recht (MMR) 2013, S. 769.

39 L. Meyer-Gossner/B. Schmitt, Beck’scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7b; S. Hegmann, in J.-P. Graf (Hrsg.), Beck’scher Online-Kommentar StPO, 27. Ed., § 110, Rn. 15.

40 N. Obenhaus, Cloud Computing als neue Herausforderung für die Strafverfolgungsbehörden und Rechtsanwaltschaft, Neue Juristische Wochenschrift (NJW) 2010, S. 651; M. Gercke, Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage, Computer und Recht (CR) 2010, S. 345-348 (347).

41 B. Gercke, in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 29.

42 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Eva Bulling-Schröter, weiterer Abgeordneter und der Fraktion DIE LINKE, Bundestgas-Drucksache 18/10763, S. 6, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/109/1810948.pdf (20.10.2017).

43 Siehe hierzu beispielsweise European Parliament, Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices – Study for the LIBE Committee, März 2017, verfügbar unter http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (08.02.2018), S. 79 *et seq*.

44 § 100b Abs. 1 Nr. 1-3 Strafprozessordnung (StPO); Voraussetzung hierfür ist, dass entweder der begründete Verdacht vorliegt, die betroffene Person sei Täter oder Teilnehmer einer der in der Norm aufgelisteten besonders schweren Straftat, dass die jeweilige Tat auch im Einzelfall besonders schwer wiegt und dass der Sachverhalt oder der Aufenthaltsort des Beschuldigten sonst nur wesentlich schwerer ermittelt werden könnte.

45 Infolge eines Urteils des Bundesverfassungsgerichts aus dem Jahr 2016[45] über mehrere Vorschriften des Bundeskriminalamtgesetzes wird das Gesetz jedoch mit Wirkung **ab 25. Mai 2018** neu gefasst. Die Online-Durchsuchung wird sodann in **§ 49** geregelt sein und im Hinblick auf einzelne Voraussetzungen detaillierter verfasst sein (abgedruckt im Bundesgesetzblatt (BGBl.) I 2017, S. 1354 *et seq*, verfügbar unter https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s

noch aus **§ 20k Bundeskriminalamtgesetz**, wonach eine solche Online-Durchsuchung zur Abwehr terroristischer Gefahren möglich ist, wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Allgemeingüter besteht, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren.[46]

Grundsätzlich sind Massnahmen der Strafverfolgungsbehörden sowie polizeiliche Massnahmen **nur im Inland** möglich, sofern eine Anwendbarkeit im **Ausland** nicht ausdrücklich geregelt ist. Unsere Recherche hat weder eine solche ausdrückliche Regelung ergeben, noch Quellen aus Rechtsprechung oder Literatur, die sich mit Fällen befasst, in denen die Online-Durchsuchung im Ausland gespeicherte Daten betrifft. Inwiefern die Online-Durchsuchung auf Grundlage der Strafprozessordnung oder des Bundeskriminalamtgesetzes **auf im Ausland gespeicherte Daten anwendbar** ist, **kann daher nicht beantwortet werden**.

1.3. Internationales und Europäisches Recht

Die **Cybercrime-Konvention** wurde von Deutschland am 9. März 2009 ratifiziert und ist am 1. Juli 2009 in Kraft getreten.[47]

Der Fernzugriff auf **offen zugängliche Daten** ist durch **Artikel 32 Buchstabe a) Cybercrime-Konvention** möglich. Die deutsche Rechtslehre erkennt darin vorgesehene Recht auch unabhängig von der Cybercrime-Konvention als Gewohnheitsrecht an und damit als ungeschriebenes und dennoch bindendes Recht.[48] Damit wäre der Zugriff auf offen zugängliche Daten nicht nur im Anwendungsbereich der Cybercrime-Konvention, sondern auch für Nicht-Vertragsstaaten erlaubt.

Für im Ausland gespeicherte **zugangsgeschützte Daten** ist gemäss **Artikel 32 Buchstabe b) Cybercrime-Konvention** ein Zugriff erlaubt, wenn der **Betroffene seine rechtmässige und freiwillige Zustimmung** gibt.[49] Allerdings kann nach **Artikel 29 Cybercrime-Konvention** zur **Vermeidung von Beweisverlust** eine umgehende Sicherung der Daten erfolgen.[50]

0037.pdf%27%5D#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl117s1354.pdf%27%5D_1516956974993 (08.02.2018)).
Zum Urteil des Bundesverfassungsgerichts: Urteil vom 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09. Siehe hierzu auch die Pressemitteilung des Bundesverfassungsgerichts vom 20.04.2016, verfügbar unter http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-019.html (08.02.2018).

46 § 20k Abs. 1 S. 1, 2 Bundeskriminalamtgesetz (BKAG).

47 Der aktuelle Stand der Ratifizierungen ist verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185 (16.10.2017). Die Cybercrime-Konvention muss von den ratifizierenden Mitgliedstaaten jeweils noch in nationales Recht umgesetzt werden, was in Deutschland durch die Gesetzesänderung Bundesgesetzblatt (BGBl) I S. 3198 mit Wirkung vom 01.01.2008 geschah.

48 B. Gercke, in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 27; L. Meyer-Gossner/B. Schmitt, Beck'scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7a.

49 B. Gercke, in B. Gercke *et al*. (Hrsg.), Heidelberger Kommentar – Strafprozessordnung, 5. Aufl., München 2012, § 110, Rn. 28; L. Meyer-Gossner & B. Schmitt, Beck'scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7a; W. Bär, Transnationaler Zugriff auf Computerdaten, Zeitschrift für Internationale Strafrechtsdogmatik 2011, S. 55.

50 Art. 25 Abs. 3 Cybercrime-Konvention (CCC). M. Tsambikakis, in V. Erb *et al*. (Hrsg.), StPO Band 3, 26. Aufl., Berlin 2014, § 110, Rn. 9 (der Autor spricht fälschlicherweise von Art. 25 Abs. 2 CCC); L. Meyer-Gossner & B. Schmitt, Beck'scher Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7a.

Die oben genannten Grundsätze gelten auch für Daten von im Ausland ansässigen **Mutter- oder Tochterunternehmen** inländischer Firmen.[51]

Die Herausgabe elektronischer Beweismittel wird auch durch die **Richtlinie über die Europäische Ermittlungsanordnung (RL EEA)**[52] erleichtert, welche das Erlangen von Beweismitteln in einem anderen Mitgliedstaat erleichtert (s. dazu ausführlich unter A.).[53]

2. Geplante Neuregelung

Unsere Recherche hat keine geplanten Neuerungen des deutschen Rechts ergeben in Bezug auf den Zugriff nationaler Strafbehörden auf im Ausland gespeicherte elektronische Daten.

Der Zugriff der nationalen Strafbehörden auf im Ausland gespeicherte Daten wird sowohl im **Europarat** wie auch in der **Europäischen Union** diskutiert (s. dazu oben, unter A.).

Im Rahmen der aktuellen Überlegungen innerhalb der EU hat die Bundesregierung Deutschland der Europäischen Kommission den Vorschlag unterbreitet, die Richtlinie über die Europäische Ermittlungsanordnung um eine Vorschrift zur **grenzüberschreitenden Sicherung elektronischer Daten** ohne technische Hilfe zu ergänzen, wie dies bereits für die Überwachung von Telekommunikationsverkehr ohne technische Hilfe vorgesehen ist.[54] Ähnlich wie in den in Artikel 31 der Richtlinie über die Europäische Ermittlungsanordnung (RL EEA) geregelten Fällen der direkten grenzüberschreitenden Telekommunikationsüberwachung erscheine es auch in Fällen der grenzüberschreitenden Sicherung gespeicherter Daten überlegenswert, zwischen den Mitgliedstaaten der Europäischen Union ein Verfahren einzuführen, bei dem der ermittelnde Mitgliedstaat den von der Massnahme betroffenen Mitgliedstaat nachträglich von der Massnahme unterrichtet und der unterrichtete Mitgliedstaat sodann widersprechen kann, falls eine entsprechende Massnahme nach seinem eigenen Recht nicht zulässig wäre.[55]

---

51 L. Meyer-Gossner & B. Schmitt, Beck'sche Kurzkommentar Strafprozessordnung, 60. Aufl., München 2017, § 110, Rn. 7a.

52 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen. Diese Richtlinie wurde von Deutschland durch das Vierte Gesetz zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen vom 05.01.2017 mit Wirkung am 22.05.2017 umgesetzt.

53 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Eva Bulling-Schröter, weiterer Abgeordneter und der Fraktion DIE LINKE, Bundestags-Drucksache 18/10948, S. 6, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/109/1810948.pdf (20.10.2017). In der Richtlinie über die Europäische Ermittlungsanordnung (RL EEA) werden klare Fristen für die Beweiserhebung vorgegeben, die Ablehnungsgründe begrenzt und der Verwaltungsaufwand durch Einführung eines einheitlichen Standardformulars verringert. Es scheint juristisch noch nicht geklärt zu sein, ob die Richtlinie nur für Anbieter gilt, die ihren Sitz in der Europäischen Union haben, oder auch für solche, die lediglich ihren Server dort betreiben.

54 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Inge Höger, weiterer Abgeordneter und der Fraktion DIE LINKE, Bundestags-Drucksache 18/11578, S. 1, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/115/1811578.pdf (20.10.2017).

55 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Inge Höger, weiterer Abgeordneter und der Fraktion DIE LINKE, Bundestags-Drucksache 18/11578, S. 5, verfügbar unter http://dipbt.bundestag.de/dip21/btd/18/115/1811578.pdf (20.10.2017).

3. Strafbarkeit ausländischer Strafverfolgungsbehörden bei direktem Zugriff auf inländische Daten

Es gibt keine einschlägige Gesetzesnorm, welche den Direktzugriff von ausländischen Strafverfolgungsbehörden auf in Deutschland gespeicherte Daten für strafbar erklärt. Nach § 9 Absatz 1 Strafgesetzbuch (StGB) ist *„[e]ine Tat […] an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte.*“ Die deutschen Strafbestimmungen wie das Ausspähen von Daten (sogenanntes „*Hacking*“)[56] könnten also anwendbar sein.[57] Neben den deutschen Strafbestimmungen würde ein solcher Direktzugriff von ausländischen Strafverfolgungsbehörden auch die territoriale Souveränität Deutschlands verletzen und somit eine Völkerrechtsverletzung darstellen.

C. AUTRICHE

1. Zugriff der Strafverfolgungsbehörden auf im Ausland gespeicherte Daten

In den österreichischen Bundesgesetzen findet sich mit **§ 111 Strafprozessordnung** lediglich eine Rechtsgrundlage für den **Zugriff auf im Inland gespeicherte elektronische Daten**.

Auf **im Ausland gespeicherte elektronische Daten** ist der Zugriff nur bedingt möglich, nämlich lediglich im Rahmen des **Artikel 32 Cybercrime-Konvention** über die **Weitergabe zugangsgeschützter Daten** und des **Artikel 29 Cybercrime-Konvention** zur **umgehenden Beweissicherung**. Zudem erlaubt das **Völkergewohnheitsrecht** in Einklang mit der Cybercrime-Konvention **Zugriff auf offen zugängliche Daten**.[58]

Eine **Direktanfrage** durch die Strafverfolgungsbehörden bei ausländischen Providern scheint nicht gesetzlich geregelt zu sein.[59]

1.1. Zugriff auf im Inland gespeicherte elektronische Daten

Die Sicherstellung und Durchsuchung von im **Inland** gespeicherten elektronischen Daten ist durch **§ 111 Absatz 2 Strafprozessordnung (StPO)** geregelt:

> *„Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.“*

---

56 §202a Strafgesetzbuch (StGB).

57 Das deutsche Strafrecht gilt auch, unabhängig vom Recht des Tatortes, für das Ausspähen von Daten in Zusammenhang mit der Verletzung von Betriebs- und Geschäftsgeheimnissen deutscher Betriebe oder Unternehmen (§ 202a Strafgesetzbuch (StGB) in Verbindung mit § 5 Nr. 7 Strafgesetzbuch (StGB)).

58 Siehe hierzu unter Punkt 1.2. in diesem Gutachten zum österreichischen Recht.

59 Siehe hierzu unter Punkt 1.3. in diesem Gutachten zum österreichischen Recht.

Ist der Zugang zu den digital gespeicherten Daten durch **Passwörter** oder sonstige Zugangsschlüssel geschützt, müssen diese von der Sicherstellung betroffenen Person grundsätzlich preisgegeben werden.[60] Dies gilt jedoch nicht für Beschuldigte und schweigeberechtigte Zeugen.[61]

1.2. Zugriff auf im Ausland gespeicherte elektronische Daten

Sind die gesuchten externen Daten auf Servern abgelegt, die sich im **Ausland** befinden, bedarf ein Fernzugriff österreichischer Behörden, auch wenn er von Österreich aus erfolgt, grundsätzlich **eines förmlichen Rechtshilfeersuchens**.[62]

Darüber hinaus ist ein grenzüberschreitender Fernzugriff auf im **Ausland** gespeicherte Daten nur unter bestimmten Voraussetzungen gestattet, welche sich in der von Österreich umgesetzten **Cybercrime-Konvention**[63] und im **Völkergewohnheitsrecht** finden.

1.3. Direktanfrage bei ausländischen Providern

Unsere Recherche hat keine Informationen dazu ergeben, inwiefern eine Direktanfrage durch die Strafverfolgungsbehörden bei ausländischen Providern möglich ist. Wir gehen daher davon aus, dass eine freiwillige Zusammenarbeit seitens der Provider mit den jeweiligen Strafverfolgungsbehörden gestattet ist, dass es jedoch keine entsprechende Verpflichtung gibt. Im Fall der Zusammenarbeit wird jedoch die Person, deren Daten betroffen sind, zu benachrichtigen sein.[64]

2. Geplante Neuregelung

Unsere Recherche hat keine geplanten Neuerungen des österreichischen Rechts ergeben in Bezug auf den Zugriff nationaler Strafbehörden auf im Ausland gespeicherte elektronische Daten.

Insbesondere scheint der österreichische Gesetzgeber noch nicht die Richtlinie über die Europäische Ermittlungsanordnung umgesetzt zu haben.[65]

3. Strafbarkeit ausländischer Strafverfolgungsbehörden bei direktem Zugriff auf inländische Daten

Im österreichischen Recht scheint es **keine Strafvorschrift** zu geben, die explizit den Zugriff durch ausländische Strafverfolgungsbehörden auf in Österreich gespeicherte Daten regelt. Unsere Recherche hat auch keine andere Strafvorschrift ergeben, die in einem solchen Fall einschlägig sein könnte. So

---

60 A. Tipold & I. Zerbes, in H. Fuchs & E. Ratz (Hrsg.), Wiener Kommentar zur Strafprozessordnung, 239. Lieferung, Wien 2015, § 111, Z 13; C. Kroschl, in G. Schmölzer & T. Mühlebacher (Hrsg.), StPO, Wien 2013, § 111, Z 11; A. Venier, in C.Bertel & A. Venier (Hrsg.), Kommentar zur StPO, Wien 2012, § 111, Z 2.

61 C. Kroschl, in G. Schmölzer & T. Mühlebacher, StPO, Wien 2013, § 111, Z 11.

62 A. Tipold & I. Zerbes, in H. Fuchs & E. Ratz (Hrsg.), Wiener Kommentar zur Strafprozessordnung, 239. Lieferung, Wien 2015, § 111, Z 14/3.

63 Die Cybercrime-Konvention wurde von Österreich am 13. Juni 2012 ratifiziert und ist am 1. Oktober 2012 in Kraft getreten, Bundesgesetzblatt (BGBl.) III 140/2012. Der aktuelle Stand der Ratifizierungen ist verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185 (08.01.2018). Siehe hierzu auch C. Bergauer, Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012, S. 205.

64 Vgl. A. Tipold & I. Zerbes, in H. Fuchs & E. Ratz (Hrsg.), Wiener Kommentar zur Strafprozessordnung, 239. Lieferung, Wien 2015, § 111, Z 17 f.

65 EUR-Lex Access to European Union Law, National Transposition, http://eur-lex.europa.eu/legal-content/FR/NIM/?uri=celex:32014L0041 (17.01.2018).

scheint der Tatbestand des **Widerrechtlichen Zugriffs auf ein Computersystem gemäss § 118a Strafgesetzbuch (StGB)** lediglich auf **Inlandstaten** Anwendung zu finden.[66] **§ 124 Strafgesetzbuch über die Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslandes**[67] hingegen betrifft ausschliesslich Fälle von sogenanntem **wirtschaftlichem Landesverrat** und erfasst daher lediglich Wirtschaftsgeheimnisse.

D. BELGIQUE

1. Accès par les autorités pénales aux données stockées à l'étranger

1.1. Panorama général

En matière d'entraide pénale, la Belgique est partie aux différents instruments de droit européen pertinents (cf. 1.3) et a conclu en sus différents accords bilatéraux avec des pays tiers[68], lesquels régissent la coopération entre les autorités pénales belges et étrangères.

Par ailleurs, le droit belge, sous l'impulsion de la Cour de cassation suivie par le législateur il y a peu[69], **permet aux autorités belges d'accéder, dans une certaine mesure directement, à des données stockées à l'étranger**. En ce sens, le critère déterminant repris dans le Code d'instruction criminelle (ci-après : C.i.cr) pour se voir appliquer les dispositions pertinentes, et notamment l'art. 90*ter* relatif aux contenus-mêmes, peut-être résumé ici comme étant le fait **d'offrir ou de mettre à disposition, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques**[70].

La Belgique a ainsi vu son droit interne évoluer de telle sorte à le rendre plus adapté à un monde connecté, allant, par essence, au-delà du strict principe de territorialité.

Avant d'analyser en détail la question centrale des compétences personnelle et territoriale des autorités belges en présence de données à l'étranger, au regard de la jurisprudence et des récentes modifications législatives (1.3), il sied de présenter les différentes possibilités d'action de l'autorité de poursuite pénale quant à l'accès à certaines données en général, celles-ci étant prévues par le Code d'instruction criminelle (1.2).

---

66 Vgl. §§ 62-65 Strafgesetzbuch (StGB), welche keine Strafbarkeit für im Ausland begangene Taten im Sinne des § 118a StGB begründen.

67 § 64 Abs 1 Z 1 Strafgesetzbuch (StGB) sieht ausdrücklich die Strafbarkeit im Ausland begangener Taten im Sinne des § 124 StGB vor.

68 Cf. par exemple, Convention entre le Royaume de Belgique et les Etats-Unis d'Amérique concernant l'entraide judiciaire en matière pénale, signée le 28 janvier 1988 (version conforme à l'Accord entre l'Union européenne et les Etats-Unis d'Amérique du 25.06.2003), disponible sous : http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl (06.02.2018)

69 Cf. Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales (ci-après : Loi du 25 décembre 2016), publiée au Moniteur belge le 17.01.2017, entrée en vigueur le 27.01.2017, et disponible sous : http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=17-01-17&numac=2017030017 (09.01.2018).

70 Cf. en particulier l'art. *90ter* C.i.cr mais ég. l'art. 46*bis* § 1, al. 2 et 88*bis* C.i.cr.

1.2. Les moyens d'action de l'autorité de poursuite pénale

1.2.1. L'identification de l'utilisateur d'un moyen de communication électronique (art. 46*bis* C.i.cr.)

Aux termes de l'art. 46*bis* C.i.cr., **le procureur du Roi**, peut, par décision motivée, requérir le concours d'opérateurs de réseau de communications électroniques dans le but d'obtenir certaines données d'identification[71]. Cette disposition permet d'obtenir non seulement **l'identité et les coordonnées de l'abonné ou de l'utilisateur habituel d'un service de télécommunication**[72] **mais également les moyens de communication auxquels une personne déterminée est abonnée ou qu'elle utilise régulièrement**[73]**.** Les données concernent ici principalement une cible ou une personne sans qu'un aperçu historique des communications électroniques ne puisse être demandé[74]. L'art. 46*bis* C.i.cr permet ainsi d'obtenir, entre autres, **l'identité d'un titulaire d'une adresse mail** auprès d'un fournisseur d'accès, ou encore **l'identité de l'utilisateur d'un réseau internet**, à partir d'une adresse IP fixe[75].

En conformité avec la Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (ci-après : Loi du 29 mai 2016)[76], l'art. 46*bis*, § 1er, al. 5 C.i.cr. pose une limite en ce sens que lorsque les infractions ne sont pas de nature à entraîner un emprisonnement d'un an ou plus, le procureur du Roi peut requérir les données portant uniquement sur **une durée maximale de 6 mois** préalable à sa décision.

Les opérateurs ou fournisseurs de réseau visés par la mesure ont un **devoir de collaboration** (cf. ci-dessous 1.3) : ils doivent communiquer au procureur du Roi ou à l'officier de police les données « **en temps réel ou le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi** […][77]. La personne qui ne se conformerait pas à ce devoir se voit exposé à une amende de 26 à 10'000 euros[78].

1.2.2. Le repérage et la localisation de communications électroniques (art. 88*bis* C.i.cr)

En vertu de l'art. 88*bis* C.i.cr, le **juge d'instruction** a la possibilité de faire procéder « au repérage des données de trafic de moyens de communications électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées[79] » et « à la localisation de

---

71 C. Forget, La collecte de preuves informatiques en matière pénale, in J.-F Henrotte et F. Jongen (dir.), Pas de droit sans technologie, Larcier, Bruxelles 2015, p. 265.

72 Art. 46*bis*, § 1er, al. 1, 1er tiret C.i.cr.

73 Art. 46*bis*, § 1er, al. 1, 2ème tiret C.i.cr; A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, in C.-E. Clesse, Droit pénal de l'entreprise 2017/3, Larcier, Bruxelles 2017, p. 181 ss.

74 C. Forget, La collecte de preuves informatiques en matière pénale, *op. cit*., p. 265, avec références, notamment à J. Kerkhofs et P. Van Linthout, Artikel 46bis van het Wetboek van strafvordering en de motiveringsfplicht : de minimis non curat praetor? T. Straf., 2011/6, p. 428, disponible uniquement en néerlandais ; voir ég. A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit.*, p. 182 reprenant la même source.

75 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit.*, p. 182.

76 Publiée au Moniteur belge le 18.07.2017 et entrée en vigueur le 28.07.2016, le texte est disponible sous : http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl (10.01.2018)

77 Art. 46*bis*, § 2 C.i.cr.

78 Art. 88*bis*, § 2, al. 4 C.i.cr.

79 Art. 88*bis*, § 1, al. 1er, 1° C.i.cr.

l'origine ou de la destination de communication électronique[80] ». Les données concernées ici sont multiples et portent entre autres, sur l**e jour, l'heure, la durée, le correspondant et la localisation de la communication électronique**[81]**, mais nullement sur le contenu-même de cette dernière**[82]. Dans tous les cas, une mesure sur la base de l'art. 88*bis* C.i.cr peut être ordonnée uniquement lors de la poursuite d'une infraction passible d'un emprisonnement d'au moins 1 an[83].

Pour ce qui est du devoir de collaboration, l'art. 88*bis*, § 4, al. 1 reprend la même formulation que l'art. 46*bis*, § 2 C.i.cr. (cf. 1.2.1) : « **toute personne qui refuse de prêter son concours technique aux réquisitions** » ou **ne le prête pas en temps réel ou au moment défini par la demande**, sera punie d'une amende de 26 à 10'000 euros[84].

1.2.3. L'interception, la prise de connaissance, l'exploration et l'enregistrement de communications non accessibles au public ou des données d'un système informatique (art. 90*ter* et suiv. C.i.cr)

L'art. 90*ter* et suivants C.i.cr permettent **au juge d'instruction** « d'intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, **des communications non accessibles au public ou de données d'un système informatique** ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci[85]» et ce dans le secret.

Les « communications non accessibles au public ou de données d'un système informatique ou d'une partie de celui-ci » correspondent à « tout énoncé oral ou non oral fait directement ou à distance, et notamment les déclarations et conversations directes ou téléphoniques, de même que **toutes les formes modernes de la télématique** » et s'étend tant aux données vocales, textes ou encore aux images[86].

C'est par le biais de cette mesure que peuvent être obtenus les **contenus de communications électroniques privés**, si besoin en requérant la collaboration des opérateurs ou des fournisseurs du service de communications en question, laquelle pourra être demandée sur la base de **l'art. 90*quater*, § 2 C.i.cr[87].**

L'article 90*quater* § 2 (relatif à l'accès aux contenus) se lit comme suit[88]:

> *« Afin de permettre la mesure visée à l'article 90ter, § 1er, le juge d'instruction peut requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, le concours:*
>
> *- de l'opérateur d'un réseau de communications électroniques;*

---

80 Art. 88*bis*, § 1, al. 1er, 2° C.i.cr.

81 À noter que le terme « appel » a été remplacé par « communication électronique » lors de l'adoption de la Loi du 29 mai 2016 afin d'englober les communications par le biais d'Internet.

82 Cf. ég. art. 88 *bis*, § 1, al. 5 et § 2 C.i.cr. pour d'avantage de détails sur les durées autorisées en fonction de la gravité des infractions.

83 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit.*, p. 184.

84 Art. 88*bis*, § 2, al. 3 C.i.cr.

85 Art. 90*ter*, § 1er, al. 1er C.i.cr.

86 Selon la formulation de la Cour de cassation belge : C. Cass., 26 mars 2003, n° P030412F, disponible sous : https://app.vlex.com/#vid/38150719 (25.01.2018)
A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit.*, p. 182.

87 Art. 90*quater* § 1er C.i.cr. : « Toute mesure sur la base de l'art. 90*ter* fait l'objet d'une autorisation écrite et motivée du juge d'instruction ».

88 Dans sa nouvelle teneur (Loi du 25 décembre 2016).

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques ».

De plus, la nouvelle législation prévoit désormais que le procureur du Roi peut, **dans les cas d'extrême urgence,** donner un accord verbal à la mise en place des trois mesures présentées ci-dessus, moyennant un accord écrit et motivé subséquent[89].

Suivant le principe de proportionnalité, la loi restreint néanmoins le champ d'application de cette mesure en ne l'autorisant que pour **certains types d'infractions listées** à l'art. 90*ter* 2 à 5 C.i.cr., parmi lesquelles figurent le terrorisme, les crimes d'ordre sexuel, ou encore le crime organisé[90]. Enfin, selon l'art. 90*quater*, 1er, 4° C.i.cr., **cette mesure ne peut pas être ordonnée pour une durée de plus d'un mois, avec un renouvellement possible si la durée maximale n'excède pas 6 mois**[91].

Une personne qui refuserait de prêter son concours technique aux réquisitions visées aux alinéas 1er et 2 sera punie d'un **emprisonnement de six mois à un an et d'une amende de 26 euros à 20'000 euros** ou d'une de ces peines seulement, selon l'art. 90*quater*, § 4, al, 3 C.i.cr.

1.3. Le devoir de collaboration des fournisseurs étrangers

La question des **champs d'application personnel et territorial des devoirs de collaboration** des art. 46*bis*, 88*bis* et 90*quater* C.i.cr décrits ci-dessus (cf. 1.2) est centrale afin de déterminer dans quelle mesure une autorité belge peut avoir accès à des données stockées à l'étranger. La Cour de cassation belge s'est prononcée plusieurs fois sur cette thématique, lors de la saga judiciaire dite « *Yahoo* », laquelle opposait la firme américaine aux autorités pénales belges qui avaient directement requis la collaboration de *Yahoo*, sur la base de l'art. 46*bis* C.i.cr afin d'obtenir, **notamment des identifiants e-mails, ainsi que toute autre information personnelle liée aux comptes** d'auteurs présumés d'infractions, à l'exclusion cependant du contenu des correspondances[92].

Dans une dernière décision datée du 1er décembre 2015[93], la Cour de cassation a estimé que **toute entreprise offrant des services de communications électroniques sur le territoire belge était soumise aux différents devoirs de collaboration** (art. 46*bis*, 88*bis* et 90*quater*). Par ailleurs, toujours selon elle, une entreprise offre ses services sur le territoire belge « **lorsqu'elle oriente activement ses activités économiques vers des consommateurs en Belgique**[94] ». À ce titre, certains indices peuvent être déterminants, tels que l'existence d'un nom de domaine « .be », l'usage du néerlandais ou du français,

---

89 Art. 46*bis*, § 1, al. 4, 88*bis*, § 1, al. 9 et 90*quater*, § 1, al. 2 C.i.cr.

90 Force est de constater que la liste s'est élargie à bien d'autres infractions, et ne revêt plus un caractère proprement limitatif. Il peut être renvoyé à la disposition en question pour une liste exhaustive.

91 Art. 90*quinquies*, al. 1er C.i.cr.

92 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit.*, p. 186.

93 C. Cass, 1er décembre 2015, n° P.13.2082.N, disponible sous : https://juricaf.org/arret/BELGIQUE-COURDECASSATION-20151201-P132082N (11.01.2018); cette affaire s'est caractérisée par plusieurs aller-retours entre différentes Cours d'appel et la Cour de cassation de telle sorte que nous nous limiterons à cette unique décision finale. Les références des autres décisions sont les suivantes : C. Cass., 18 janvier 2011, n° P.10.1347.N, disponible sous : https://lex.be/fr/doc/be/jurisprudence-belgique/cour-de-cassation-arret-18-janvier-2011-bejc_201101181_fr (25.01.2018) et C. Cass., 4 septembre 2012, n° P.11.1906.N, disponible sous : https://lex.be/fr/doc/be/jurisprudence-belgique/cour-de-cassation-arret-4-septembre-2012-bejc_201209046_fr. (25.01.2018)

94 C. Cass, 1er décembre 2015, *op. cit.*, point 8.

la publicité ciblée ou encore l'existence d'une boîte aux réclamations en ligne adressée aux utilisateurs belges[95].

Par cette interprétation large du devoir de collaboration, **Yahoo fut contraint d'accéder de manière directe aux demandes des autorités belges, en vertu de l'art. 46*bis* C.i.cr** (sans cependant que cela ne concerne *in casu* les contenus à proprement parler)**, et en l'absence de commission rogatoire,** par exemple.

Le champ d'application personnel des articles 88*bis* et 90*quater* C.i.cr. (relatif à l'accès aux données-mêmes) étant alors défini de manière identique à celui de l'art. 46*bis* C.i.cr., l'enseignement de l'affaire Yahoo a pu être transposé à ces deux dispositions[96].

Ainsi, dans une décision plus récente et concernant cette fois-ci **l'accès aux données-mêmes des correspondances**, le Tribunal correctionnel d'Anvers a rejoint la position de la Cour de cassation en condamnant l'entreprise américaine **Skype**, sur la base cette fois des **art. 88*bis* et 90*quater* C.i.cr**[97]. Dans cet arrêt, le Tribunal a rejeté un argument supplémentaire de Skype qui invoquait une impossibilité de décrypter les données en cause ne lui permettant pas de collaborer. La Cour a estimé que l'entreprise avait créé elle-même cette situation et qu'il lui revenait de procéder au décryptage afin de respecter son devoir de collaboration[98].

Prenant en compte ces développement jurisprudentiels, le législateur a récemment adopté la Loi du 25 décembre 2016 déjà citée, qui **adapte et précise d'un point de vue personnel et territorial les devoirs de collaboration pertinents, fournissant ainsi une possibilité d'accès direct aux autorités pénales belges, en particulier à l'art. 90*quater* § 2 C.i.cr présenté ci-dessus.**

À noter que **les art. 46*bis*, § 1, al. 2 et 88*bis*, § 1, C.i.cr.** présentés ci-dessus contiennent **des formulations identiques**, permettant ainsi également de requérir le concours d'acteurs étrangers.

À noter encore que le texte explicatif du Parlement accompagnant le projet de loi du 25 décembre 2016 **mentionne explicitement des entreprises comme Yahoo Mail, Hotmail, Gmail, Facebook, Twitter, WhatsApp ou Instagram**, en indiquant que cette nouvelle catégorie de fournisseurs doit s'interpréter au sens large et que l'obligation de coopération prévues aux trois articles susmentionnés s'impose également à ces acteurs étrangers[99].

En ce qui concerne les cas où, pour faire application de l'article 90*ter* et suivants C.i.cr permettant au juge d'instruction d'accéder au contenu des communications électroniques, **la collaboration des fournisseurs de service ne serait pas nécessaire**, le droit positif belge ne dit pas si l'accès à des données stockées à l'étranger serait possible.

---

95 *Idem*, p. 9.

96 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit*., p. 185.

97 Corr. Anvers, 27 octobre 2016, NC, 2017.

98 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit*., p. 192.

99 Chambre des représentants de Belgique, projet de loi du 8 juillet 2016 relatif à l'amélioration des méthodes particulières de recherche de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, exposé des motifs, DOC 54 1966/001, disponible sous : http://www.lachambre.be/FLWB/PDF/54/1966/54K1966001.pdf (10.01.2018)

1.4. Droits européen et paneuropéen

La Belgique a ratifié la **Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercrimalité**, le 20 août 2012, cette dernière étant entrée en vigueur en Belgique le 1er décembre 2012[100].

En ce qui concerne l'Union européenne, la **Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale** a été transposée en droit belge par la Loi du 22 mai 2017 relative à la décision d'enquête européenne en matière pénale[101].

2. Réformes prévues

Comme présenté ci-dessus, des réformes sont déjà intervenues récemment dans ce domaine. Il n'y a pas de nouvelle réforme prévue à notre connaissance.

3. Punissabilité de l'accès direct par une autorité pénale étrangère à des données stockées sur le territoire national

En matière d'obligation de collaboration des fournisseurs de service (cf. 1.3.), le **principe de réciprocité** conduirait à ce que Belgique accepte que des autorités judiciaires étrangères s'adressent directement à des entreprises belges pour obtenir leur collaboration[102].

Le droit belge protège de manière générale le contenu des communications électroniques, en tant qu'il s'agit d'une composante de la **vie privée**, en particulier à l'art. 124 de la Loi du 13 juin 2005 relative aux communications électroniques[103] ainsi que l'art. 259 du **Code pénal qui punit les autorités publiques** ; ce dernier dispose[104] :

> *« § 1er.Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit:*
>
> *1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications;*
>
> *2o soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque;*
>
> *3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.*

---

100 L'état des ratifications peut être consulté ici : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ITUAhWZ6 (10.01.2018).

101 Publiée au Moniteur belge le 23 mai 2017, entrée en vigueur le même jour, disponible sous : http://www.ejustice.just.fgov.be/eli/loi/2017/05/22/2017012230/moniteur (10.01.2018).

102 A. Gossé, Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ?, *op. cit*., p. 203.

103 Publiée au Moniteur belge le 20 juin 2005, entrée en vigueur le 30.06.2005 et disponible sous : http://www.ejustice.just.fgov.be/eli/loi/2005/06/13/2005011238/justel (07.02.2018)

104 Cf. ég. l'art. 314*bis* du Code pénal qui contient une disposition similaire ne se limitant pas aux agents de l'Etat (« quiconque »). Voir ég. les art. 22 de la Constitution belge et 8 CEDH protégeant tous deux la vie privée.

§ 2 sera puni d'un emprisonnement de six mois à cinq ans et d'une amende de cinq cents [euros] à trente mille [euros] ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications non accessibles au public ou de données d'un système informatique.

§ 2bis, Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er ».

Nos recherches n'ont pas permis de **conclure à ou d'exclure l'applicabilité de ces dispositions aux autorités de poursuite pénale étrangères**. En outre, à notre connaissance, **il n'existe pas, en droit pénal belge, de disposition spécifique** punissant un accès direct d'une autorité pénale étrangère à des données stockées en Belgique.

Il peut être intéressant de mentionner **l'art. 90*ter*, § 6, C.i.cr.**, lequel s'applique cependant uniquement lorsque la personne visée par la mesure se trouve sur le territoire belge et ne fait donc pas expressément référence au stockage de données en Belgique. Cette norme dispose « qu'**une autorité étrangère compétente, peut, dans le cadre d'une enquête pénale, intercepter, prendre connaissance et enregistrer des communications non accessibles au public ou des données d'un système informatique lorsque la personne visée par cette mesure se trouve sur le territoire belge**[105]**»**.

L'art. 90*ter*, § 7 C.i.cr. prévoit que **le juge d'instruction, saisi par le procureur, autorise la mesure *a posteriori*** si les conditions sont remplies et la notifie à l'autorité étrangère dans un délai de 96 heures (sauf si un délai supplémentaire est nécessaire). Si une telle mesure n'est pas autorisée, les données interceptées doivent être détruites sans pouvoir être utilisées (art. 90*ter*, § 7, al. 5 C.i.cr).

E. ETATS-UNIS

1. Access of Criminal Prosecution Authorities to Data Stored Abroad in Electronic Messages and on Social Networks

In order for U.S. law to be relevant to the answer to this question, U.S. law must apply to the request for access. In the case of a U.S. law enforcement authority, this would be unlikely unless a person located in the U.S. has "possession, custody or control"[106] of the data requested. In such a case, U.S. law enforcement would most likely be required to obtain a warrant, which would be subject to a Constitutional law analysis. If the request is to be made to a person outside the U.S., only U.S. law with extraterritorial effect may apply, otherwise the international mutual assistance procedures would apply. If the request is made by a foreign law enforcement authority, ordinarily, the mutual assistance procedure would be the appropriate channel.
U.S. law will not have extra-territorial effect unless the legislature specifically intended the provision in question, when it was enacted, to apply internationally. Moreover, U.S. courts can order a party located outside the jurisdiction to produce information only where the court has personal jurisdiction of such party. Nonetheless, even if a court cannot exercise jurisdiction over an absent party, it may

105 Cf. l'art. 90*ter* § 6 C.i.cr. pour les conditions d'application de cette disposition.

106 See discussion in the following paragraphs.

nevertheless compel **access to information in the hands of the absent party where another party, subject to the court's jurisdiction, has, through the absent party, "possession, custody, or control"**[107] **of the information**. Therefore, "the test for production of documents is control, not location."[108] U.S. courts have interpreted the concept of control "broadly as the legal right, authority, or practical ability to obtain the materials sought upon demand."[109] As a result of "the broad judicial interpretations of that standard, the U.S. government could (at least in theory) obtain information from a U.S.-based cloud service provider - including records related to foreign customers - without any notice to those customers."[110] Moreover, according to this analysis of "possession, custody, or control," U.S. courts have, on many occasions, ordered the production of information in the possession of foreign entities, where the court has jurisdiction over a related entity in a U.S. proceeding.[111]

The Second Circuit federal Court of Appeals, in ***Matter of a Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp***[112]*,* the only appellate decision to date, has ruled that Microsoft was not required to repatriate information stored on a server in Dublin, Ireland, because to do so would be an impermissible extraterritorial application of the Stored Communications Act ("SCA")[113] This case has been appealed to the U.S. Supreme Court, which agreed to hear the case (granted *cert.)* in October of this year[114]. In the interim, five cases have held that disclosure of electronic information in the United States retrieved from computers abroad does not constitute an extraterritorial application of the SCA.[115] Under U.S. law, as mentioned above, federal legislation does not apply extraterritorially unless Congress specifically intended that it so apply when the legislation was adopted.[116] In at least one case, the U.S. government has argued that Senate ratification of the

---

107 Federal Rules of Criminal Procedure 16(b)(1).

108 *Dietrich v. Bauer*, 2000 WL 1171132 at *2 (S.D.N.Y. Aug. 16, 2000) (quoting *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983)). See, also, *Afros S/P.A. c. Krauss-Maffei Corp.*, 113 F.R.D. 127, 129 (D. Del. 1986) ("personal jurisdiction and 'control' of documents are distinct issues in that [the] court can compel discovery of documents in [the] 'control' of a party although in 'possession' of a person over whom there is no personal jurisdiction.")

109 See *Bank of New York v. Meridien Biao Bank Tanzania*, 171 F.R.D. 135, 146 (S.D.N.Y. 1977); see also *Goodman v, Praxair Servs. Inc*., 632 F. Supp. 494, 516 n.11 (D. Md. 2009); *In re NTL, Inc. Sec. Litig*., 244 F.R.D. 179, 195 (S.D.N.Y. 2007); *Asset Value Fund, Ltd. V. The Care Group, Inc*., 1997 U.S. Dist. LEXIS 19768 at 9 (S.D.N.Y. 1997).

110 S. C. Bennett, M. J. Daley & N. Gerlach, Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. PATRIOT ACT, 13 Sedona Conf. J. 235, 238 (2012).

111 See, e.g., *Gucci Amer., Inc. v. Curveal Fashion*, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010) (ordering party discovery from Malaysia); *AccessData Corp v. ALSTE Techs*., 2010 WL 318477, at *7 (D. Utah Jan. 21, 2010) (ordering party discovery from Germany); *In Re Cargo Shipping Srvs. Antitrust Litig*., 2010 WL 1189341, at *5 (E.D.N.Y. Mar. 29, 2010) (ordering party discovery from France).

112 829 F.3d 197, 222 (2d Cir. 2016) ("Microsoft I").

113 18 U.S.C. § 2701 *et seq*. A petition was subsequently filed requesting a rehearing *en banc* (by all of the judges in the Circuit). There was a four to four split concerning the petition. The rehearing *en banc* was therefore deinied leaving the panel opinion in place, 855 F.3d 53, 55 (2d Cir. 2017) ("Microsoft II").

114 *cert. granted sub nom. United States v. Microsoft Corp*., No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017).

115 See *In the Matter of the Search of Information Associated with [redacted]@ Gmail.com That Is Stored at Premises Controlled by Google, Inc.*, Case No. 16–mj–757 (GMH) (D.D.C. June 2, 2017) (Dkt. 32, Ex. G); *In the Matter of the Search of Content That Is Stored at Premises Controlled by Google*, Case No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In the Matter of the Search of Premises Located at [redacted] @yahoo.com*, Case No. 6:17–mj–1238 (M.D. Fla. Apr. 7, 2017) (Dkt. 6, Ex. D); *In re Information associated with one Yahoo email address/In re: Two email accounts stored at Google, Inc.*, Case No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017) (Dkt. 6, Ex. C); *In re Search Warrant No. 16–960–M–01 to Google,* 232 F.Supp.3d 708 (E.D. Pa. 2017).

116 *RJR Nabisco v. European Community*, 579 US __, 136 S. Ct. 2090, 195 L. Ed. 2d 476, (2016).

Council of Europe Convention on Cybercrime indicates Congress' intention that the SCA should apply extraterritorially. The district court of the Northern District of Alabama, however, rejected the argument, confirming the prior case law holding that the SCA does not apply outside the U.S.

In **another case**, the magistrate judge in the Northern District of California authorized a search warrant[117], under the SCA, directing Google to produce all stored content related to certain email accounts retrievable from the United States. Google refused to produce content located abroad. The parties agree that Google should be held in contempt of the order thereby enabling Google to appeal the warrant, pending the outcome of the U.S. Supreme Court decision in the *Microsoft* case.[118]

At the hearing, Google provided more information on its operating system. It stated that any transmission of data in a foreign country back to the United States would not occur by human hand but through a direction or command from Google headquarters in Mountain View, California, to servers abroad.[119] Data is distributed overseas for efficiency and optimization reasons, not because of anything that the account holder did or requested.[120] Indeed, the account holder has no expectation whether the data is abroad or in the United States.[121] Google's system operates automatically and thus a user cannot use it to put data outside the reach of U.S. law enforcement.[122] **Google's system is not controlled by an individual but by network parameters**.[123] In this respect, Google's system differs significantly from Microsoft's system, in which users enter a country code like Ireland at registration and then Microsoft migrates the data to Ireland to be stored there.[124]

The Supreme Court decision in the Microsoft case, when it is handed down, is expected to provide at least some clarity in this area. For the moment, however, oral arguments have not yet been scheduled. As such, it is unlikely that the opinion in this case will appear before **the end of the 2018 spring term**.

2. Future Reforms

The currently-existing mutual legal assistance procedures are often slow and cumbersome. In the interest of facilitating criminal investigations, in July 2016, the Department of Justice published **proposed legislation**[125] **on cross-border data, which would enable approved foreign governments to conclude executive agreements with the U.S**. Such agreements would allow the approved foreign governments to submit requests for electronic data, both stored and intercepted live, directly to U.S. companies rather than having to obtain a decision from a U.S. court, as is currently the case. The draft legislation sets out the standards countries must meet to qualify for an agreement and establishes what the requests can include. For example, requests must pertain to a serious crime, including terrorism. **This proposal would also afford the U.S. reciprocal rights with respect to the partner**

---

117 *In re Search of Information Associated with Accounts Identified as [redacted]@gmail.com and others Identified in Attachment A that are Stored at Premises Controlled by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94025,* 2017 WL 3263351 (C.D. Cal. 2017).

118 *Matter of the Search of Content Stored at Premises Controlled by Google Inc.,* 2017 WL 4700056 (N.D. Cal. 2017).

119 Transcript of the hearing at 30.

120 *Id*. at 31–32.

121 *Id*. at 33.

122 *Id.*

123 *Id.* at 44.

124 *Id.* at 33,44.

125 U.S. Department of Justice, "Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposed of Combating Serious Crime including Terrorism" §§ 3(a)-3(c) available at: https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf (28 November 2017)("proposed legislation").

country.[126] In addition, it would add exceptions to existing legislation to permit companies to 1) intercept and 2) disclose stored electronic communications in response to a foreign order made pursuant to an executive agreement.[127] Countries would be vetted, then, but individual orders would not be subject to U.S. government approval.[128]

Under the proposed legislation, the conditions a foreign government would be required to meet to qualify for an executive agreement would include a determination by the Attorney General and the Secretary of State that the foreign government has domestic laws that "afford robust substantive and procedural protections for privacy and civil liberties" including

- substantive and procedural laws on cybercrime and electronic evidence;
- respect for the rule of law and principles of non-discrimination,
- adherence to applicable international human rights obligations;
- mechanisms to provide accountability and transparency for data collection;
- a showing of clear mandates, procedures, and effective oversight of authorities' collection, retention, use, and sharing of data;
- mechanisms for accountability and transparency for the collection and use of data; and
- a commitment to promote and protect the free flow of information and the open Internet (essentially a promise not to pursue actions such as data localization).[129]

Under the proposed legislation once an executive agreement is in place, **the foreign country would be able to send a request to an electronic communications company directly, without first going through U.S. agencies or courts**. The request itself:

- cannot infringe freedom of speech;
- must be subject to review or oversight by a court, judge, magistrate, or other independent authority in the issuing country;
- must be based on requirements for a reasonable justification based on articulable and credible facts;
- must be issued in compliance with the foreign country's domestic law, and any obligation for a provider to produce data is solely from that law;
- not intentionally target a U.S. person (or person located in the U.S.) or target a non-U.S. person with the intention of obtaining information on a U.S. person;
- must pertain to the "prevention, detection, investigation, or prosecution of serious crime, including terrorism" and must use a specific identifier (i.e., name, account, or personal device);
- must be based on articulable and credible facts, particularity, legality, and severity of the conduct under investigation; and
- if the order is for the interception of wire or electronic communications, it must be of fixed, limited duration and can only be issued where that same information could not be reasonably obtained by a less intrusive method.[130]

---

126 *Id.*

127 *Id.*

128 T. Lin & M. Fidler, 2017, "Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement," A Berklett Cybersecurity publication, Berkman Klein Center for Internet & Society, p. 4 [internal citations omitted] available at: https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1 (28 November 2017) .

129 *Id.* at 5

130 *Id.*

The proposed legislation also contains an "anti-cat's paw"[131] provision, stating that the U.S. cannot use this agreement to ask a foreign government to share information the U.S. would not be able to obtain on its own.[132]

Additional procedural requirements would apply under the executive agreement. The foreign government must:

- promptly review all material collected, and segregate, seal or delete (may not disseminate) material not found to be relevant to the request;
- not disseminate content concerning a U.S. person to a U.S. authority unless it relates to significant harm or threat of the U.S. or U.S. persons including crimes of national security, terrorism, violent crime, child exploitation, or significant financial fraud;
- afford reciprocal rights of data access to the U.S.;
- agree to periodic reviews of compliance, with the U.S. government reserving the right to rescind the agreement.

The company would not be compelled under U.S. law to respond to the request.[133]

It should be noted that this proposal would allow foreign countries to make requests based on their own laws rather than requiring compliance with U.S. law, on the one hand and, on the other hand, would **allow U.S. companies to respond without penalty under U.S. law**, thereby resolving the conflicts of law and comity issues often posed under the current schema.

On **February 6, 2018**, Senators Hatch, Coons, Graham and Whitehouse introduced S.2383 the **Clarifying Lawful Overseas Use of Data (CLOUD) Act**[134] in the Senate. The CLOUD Act is similar to the DOJ proposed legislation and would provide for **bilateral agreements** between the U.S. and other countries (similar to the proposed U.S.- U.K. Agreement) to allow law enforcement authorities to request data stored abroad.

The bill would amend the SCA by adding a section, 18 U.S.C. 2713 as follows:

> *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 of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control,* ***regardless of whether such communication, record, or other information is located within or outside of the United States****. [emphasis added]*

This provision, if adopted, would likely render moot the decision in the Microsoft case[135].

---

131 The U.S. Supreme Court used this expression in *Staub v. Proctor Hospital*, 113 S. Ct. 1186 (Mar. 1, 2011), an employment discrimination case. The term "cat's paw" derives from a 17th century fable where a cat is duped by a monkey to steal chestnuts from a fire (whereby the innocent cat burns its paws and the wily monkey makes off with the chestnuts). In the employment setting, the term refers to situations where an innocent, unbiased decision-maker (aka the cat) is influenced into taking an adverse employment action by a biased, self-serving supervisor (aka the monkey).

132 Proposed legislation, *op. cit.* at 5.

133 *Id.* at 6.

134 No official summary of the CLOUD Act has yet been issued but, when issued, it will be available at: https://www.congress.gov/bill/115th-congress/senate-bill/2383.

135 Oral arguments in that case are scheduled for February 27, 2018. It will be possible to listen to the arguments at the end of that week at: https://www.supremecourt.gov/oral_arguments/argument_audio/2017.

Another aspect of the bill would be to **remove several blocking features** (i.e. provisions of U.S. law preventing U.S. persons from complying with lawful foreign law enforcement requests) allowing disclosure to foreign governments that have entered into executive agreements with the U.S. Such agreements would only be available where "the Attorney General, with the concurrence of the Secretary of State," determines that:

> (1) The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement";
>
> (2) The foreign government has adopted minimization procedures regarding information concerning US persons; and
>
> (3) The agreement has protections to prevent the foreign government from targeting or collecting information about US persons or persons located in the US, and to prevent the US government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.[136]

The **International Communications Privacy Act** (S. 2986[137]), introduced in May of 2016 would have allowed a governmental entity to require providers of electronic communication services or remote computing services to disclose the contents of communications in electronic storage (e.g., the cloud), even where those communications are stored outside of the United States if certain conditions for obtaining the warrant are met. The bill would have allowed a governmental entity to obtain those communications only if a court found that the governmental entity had taken all reasonable steps to establish the nationality and location of the subscriber or customer whose communications were sought and that there were reasonable grounds to believe that such subscriber or customer is a U.S. person, a person physically located within the United States, or a national of a foreign country that has a law enforcement cooperation agreement with the United States. The Department of Justice would have been required to: (1) establish a process for foreign governments to file mutual legal assistance treaty requests under the current system for obtaining access to electronic communications, and (2) publish annually information concerning those requests. The Bill, however, was not enacted in the 114th Congress[138].

This bill was re-introduced in the Senate (S. 1671[139]) on July 27, 2017 and in the House of Representatives (H.R. 3718) on September 8, 2017. The Senate bill has been referred to the Committee on the Judiciary and the House bill has been referred to the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.[140] As such, it might, still, be adopted.[141]

---

136 See: By A. K. Woods & P. Swire, The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems, Tuesday, February 6, 2018, 5:49 PM, LAWFARE available at : https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems (Feb. 13, 2018).

137 https://www.congress.gov/bill/114th-congress/senate-bill/2986 (December 4, 2017).

138 *Id.*

139 https://www.congress.gov/bill/115th-congress/senate-bill/1671?q=%7B%22search%22%3A%5B%22S.+1671%22%5D%7D&r=19 (December 4, 2017).

140 Full text available at: https://www.congress.gov/bill/115th-congress/house-bill/3718/text?q=%7B%22search%22%3A%5B%22HR+3718%22%5D%7D&r=1 (December 4, 2017).

141 There are also several bills that have been introduced in Congress but which have not yet been adopted or voted down. Each of them-proposed significant amendments to the SCA which, as we have seen, is the major legislative grounds for access to e-mails and social media.
The USA Liberty Act, (HR 3989), introduced in the House of Representatives on October 6, 2017 (Text available at: https://www.congress.gov/bill/115th-congress/house-bill/3989/text?q=%7B%22search%22%3A%5B%22hr+3989%22%5D%7D&r=1 (Nov. 20, 2017)) "would create a new framework of protections and transparency requirements to ensure intelligence gathered under Section 702 meets due process and privacy rules."(New bill seeks to ease civil liberties concerns around Section..., 2017

3. National law sanctions against direct access by foreign criminal prosecution authority to data stored within the national territory in electronic messages or on social networks

Currently, foreign law enforcement authorities wishing to access data stored in the U.S. **must do so through Mutual Legal Assistance Treaties** ("MLAT") between the U.S. and the country concerned[142].

WL 4564247). It would require warrants in criminal investigations, and, for six years, would prohibit the monitoring of communications of two individuals who are not suspects themselves, but whose communications may include a target's name or some other unique identifier such as an email address (known as "about" communications searches). No corresponding legislation has been introduced in the Senate.

The USA Rights Act was introduced in the Senate (S. 1997)(this is an abbreviation for the Uniting and Strengthening America by Reforming and Improving the Government's High-Tech Surveillance Act of 2017Text available at: https://www.congress.gov/bill/115th-congress/senate-bill/1997/text (Nov. 20, 2017)) on October 24, 2017 and in the House of Representatives (H.R. 4124) (Text available at: https://www.congress.gov/bill/115th-congress/house-bill/4124/text (Nov. 20, 2017)) the following day. The USA Rights Act would amend Section 702 of FISA to "end the warrantless searches of Americans' phone calls, emails, texts and other communications routinely swept up under a program designed to spy on foreign targets."(New bill aims to end warrantless Section 702 surveillance, 2017 WL 4784069). Like the USA Liberty Act, this legislation would prohibit "back door" and "about" searches unless intelligence agencies acquire a court order to conduct surveillance and would prevent the "reverse targeting" of U.S. citizens by requiring a warrant when surveillance of a foreign individual requires collecting the communications of someone in the United States.

The E-mail Privacy Act passed the House of Representatives (H.R. 387 (full text available at: https://www.congress.gov/bill/115th-congress/house-bill/387/text?r=263 (December 4, 2017))) and has been referred to the Judiciary Committee in the Senate (S. 1654 (full text available at: https://www.congress.gov/bill/115th-congress/senate-bill/1654/text (December 4, 2017))). This pro-privacy legislation would codify the Sixth Circuit's ruling in *U.S. v. Warshak* (631 F.3d 266 (2nd Cir. 2010) available at: http://caselaw.findlaw.com/us-6th-circuit/1063654.html (December 4, 2017)), which held that the Fourth Amendment demands that the government first obtain a warrant based on probable cause before accessing emails stored with cloud service providers. The bill, however, does not require the government to notify users when it obtains their data.

142 The current MLAT process for electronic evidence requests works as follows :

1. A foreign law enforcement agency or other investigative body desiring access to data held by a U.S. company files a request with their country's designated central processing agency, which reviews the request.
2. Once approved, the foreign country sends the request to the Office of International Affairs ("OIA") of the U.S. Department of Justice ("DOJ").
3. The OIA works with the foreign country to revise the request's format and content to meet U.S. standards.
4. Once the OIA is satisfied, OIA works with a U.S. Attorney's Office to send the request to a local U.S. magistrate judge for review.
5. The court must find that the request is in keeping with all relevant U.S. law, notably including the Fourth Amendment's probable cause standard, rules of privilege, and the Fifth Amendment. If any of these are not met, the OIA and the requesting country's agency continue to work together until the court is satisfied.
6. Once approved by the court, the request is served on the relevant company.
7. Once the company receives the request, it locates and submits the relevant evidence to the OIA.
8. The OIA reviews the evidence to ensure it meets data minimization and human rights standards.
9. Finally, the evidence is sent back to the foreign government's central processing agency, which then provides it to the original investigating team. The process takes six weeks to ten months on average, often depending on the quality of the request (that is, how to what extentmuch the originally filed request followed the required standards and how many rounds of review were required).

The Electronic Communications Privacy Act[143] ("ECPA"), (specifically, Title II of ECPA, also called the Stored Communications Act ("SCA")) **prohibits U.S. companies from sharing the content of stored electronic communications** with government entities, other than pursuant to a warrant or consent of the user. Countries ordinarily follow the MLAT process to access data held in the U.S. in order to insure compliance with these restrictions. Companies may also disclose content information voluntarily in the event of an emergency involving danger of death or serious physical injury to any person which requires disclosure without delay of information relating to the emergency.[144]

The Computer Fraud and Abuse Act ("CFAA")[145] imposes **civil and criminal liability on any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer."**[146] As the Supreme Court has opined, the statute "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly."[147] Our research revealed no specific cases of foreign government authorities being prosecuted under this act (which, presumably, would pose jurisdictional and sovereign immunity issues).

F. FRANCE

1. Accès par des autorités de poursuite pénale à des données stockées à l'étranger

1.1. Présentation générale

L'accès par des autorités de poursuite pénale françaises à des données stockées à l'étranger se fait en vertu des **règles d'entraide judiciaire internationale**, conformément à ce qui est prévu dans le Code de procédure pénale pour les perquisitions et saisies informatiques. En la matière, c'est principalement la Convention sur la cybercriminalité du Conseil de l'Europe qui s'applique.

Le droit français ne prévoit **pas explicitement la possibilité**, dans le cadre d'enquêtes pénales, **d'accéder directement aux données** contenues dans des réseaux sociaux et emails à l'étranger. Toutefois, le texte applicable aux perquisitions et saisies informatiques comporte des failles qui seront présentées ci-dessous (voir point 1.3.), sur lesquelles les autorités de poursuite pénale peuvent s'appuyer afin de justifier un accès direct à des données stockées à l'étranger. En pratique, des demandes d'accès aux données sont également faites directement à des entreprises étrangères par les autorités françaises, et la réponse à ces demandes est fonction non seulement de la situation, mais aussi de la politique de l'entreprise en la matière.

143 18 U.S.C. §§ 2701 *et seq*.

144 18 U.S.C. § 2702(b)8 ; 2702(c)(4).

145 18 U.S.C. §§1030.

146 18 U.S.C. § 1030(a)(2)(C).

147 *Musacchio v. United States*, —— U.S. ——, 136 S.Ct. 709, 713, 193 L.Ed.2d 639 (2016).

1.2. Perquisitions et saisies informatiques

Les dispositions en matière de perquisitions et saisies informatiques par les autorités de poursuite pénale pour la poursuite de crimes et délits flagrants se trouvent à l'**article 57-1 du Code de procédure pénale** (CPP)[148], inséré par la loi du 18 mars 2003[149], qui dispose :

> *« Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.*
>
> *Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial.*
>
> *S'il est préalablement avéré que ces **données**, accessibles à partir du système initial ou disponibles pour le système initial, sont **stockées dans un autre système informatique situé en dehors du territoire national**, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les **engagements internationaux** en vigueur.*
>
> *Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code.*
>
> *Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible :*
>
> *1° D'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition;*
>
> *2° De leur remettre les informations permettant d'accéder aux données mentionnées au 1°.*
>
> *A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 €. »*[150]

Conformément à l'alinéa 3 de cet article, l'accès des autorités de poursuite pénale aux données stockées à l'étranger se fait par l'**entraide pénale internationale**[151]. Les règles de coopération pénale applicables devront donc être respectées pour que cet accès soit valable, principalement la Convention sur la cybercriminalité et la Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale (voir point 1.4.). En vertu de l'article 57-1 du CPP et des engagements internationaux de la France en vigueur, les autorités de poursuite pénale qui souhaitent accéder à des données stockées à l'étranger devront donc faire une demande d'entraide ou émettre une décision d'enquête européenne.

Au-delà du simple accès, il est également prévu que les autorités de poursuite pénale peuvent **copier sur tout support** les données auxquelles elles ont ainsi accédées, et **saisir ce support** (art. 57-1, al. 4 CPP).

---

148 Le CPP est disponible sous : https://www.legifrance.gouv.fr/affichCode.do;jsessionid=45CA6E973E9EA2BC2095B882E962D1AD.tplgfr38s_2?cidTexte=LEGITEXT000006071154&dateTexte=20171130 (12.01.2018).

149 Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, art. 17, Journal officiel du 19 mars 2003.

150 Mises en évidence ajoutées.

151 S. Detraz, Fasc. 1140 : Les saisies informatiques en matière répressive, in Encyclopédie du JurisClasseur : Communication, LexisNexis, 10 Juillet 2015.

1.3. Possibilités d'accès direct

Un **accès direct aux données**, sans passer par l'entraide internationale, peut cependant être envisagé puisque la procédure d'accès énoncée à l'article 57-1 al. 3 du CPP ne s'applique que **« s'il est préalablement avéré » que les données sont stockées à l'étranger**. L'officier de police pourrait donc recueillir des données sans égard aux conventions internationales si ce n'est que par la suite qu'il découvre que ces données se trouvent à l'étranger ou si cela n'est pas certain[152]. Cet article 57-1 n'est de plus applicable qu'aux perquisitions dans le cadre d'enquêtes portant sur des crimes et délits flagrants.

C'est notamment ce qui ressort d'une décision de la chambre criminelle de la Cour de cassation en France, qui a statué en 2013 sur **une affaire où des policiers français avaient accédé à des données stockées sur un site californien depuis leur ordinateur dans leurs locaux grâce à un code récupéré lors d'une perquisition**[153]. La Cour a considéré que cette consultation de données dans les conditions précitées ne constituait qu'une investigation et non une perquisition au sens de l'article 57-1, et que « la seule domiciliation du site en cause aux Etats-Unis ne justifiait pas la mise en œuvre d'une procédure d'entraide pénale ». De plus, bien que la France et les Etats-Unis soient tous deux parties à la Convention sur la cybercriminalité, l'article 32 de ladite Convention (accès à des données sans autorisation de l'autre Etat) ne s'appliquait pas en l'espèce « dès lors qu'il ne résulte ni de l'arrêt ni des pièces de la procédure que ce texte était applicable, en l'absence de preuve que les données recherchées étaient stockées sur le territoire des Etats-Unis ». Toutefois, la situation de cette affaire était particulière car les autorités de poursuite pénale étaient déjà en possession du code d'accès, récupéré lors d'une perquisition, et donc n'ont pas eu besoin d'avoir recours aux opérateurs de télécommunications pour accéder aux données stockées.

En vertu des articles 706-102-1 et 706-102-2 du CPP, les agents de police peuvent aussi avoir un accès direct à des données en mettant en place un **dispositif technique** visant notamment à **accéder en tous lieux à des données stockées** dans un système informatique. Cet accès est mis en œuvre sans le consentement de la personne concernée. Cette **possibilité** est cependant **limitée** à des infractions graves (criminalité organisée), doit être autorisée par le juge des libertés et de la détention ou le juge d'instruction et cette autorisation est délivrée pour une durée limitée (articles 706-102-1 à 706-102-3 du CPP). Nos recherches n'ont toutefois pas permis d'établir si ces dispositions sont applicables lorsque des données sont stockées à l'étranger[154].

Bien que cela ne soit pas expressément régi par le droit national, il est également possible que des autorités de poursuite pénale **demandent directement aux entreprises étrangères** d'avoir accès ou d'obtenir des renseignements sur une personne, et la réponse à ces demandes dépend des cas et de la politique appliquée par l'entreprise. Deux exemples concernant des demandes adressées à des entreprises peuvent être cités ici. Tout d'abord, les demandes de données sur des utilisateurs à Google aux Etats-Unis doivent normalement passer par une procédure d'entraide pénale internationale, sauf dans les cas de demandes de divulgation d'urgence lorsque la fourniture de données peut prévenir des risques de mort ou de blessures graves à l'encontre d'une personne ou lorsque, sur une base volontaire, Google choisit d'accéder à la demande d'une autorité étrangère qui respecterait les

---

152 S. Detraz, Fasc. 1140 : Les saisies informatiques en matière répressive, *op. cit.*

153 Cass. crim., 6 nov. 2013, n° 12-87.130 : JurisData n° 2013-024912 ; Bull. crim. 2013, n° 217.

154 Une étude de la commission des libertés civiles, justice et affaires intérieures du Parlement européen sur les mesures de hacking dans différents Etats membres a notamment précisé que ce type de mesures comportent des risques relatifs à la souveraineté territoriale puisque les autorités ne sont pas toujours en mesure de déterminer la localisation des données. Directorate-general for Internal policies, Legal Frameworks for hacking by law enforcement : identification, evaluation and comparison of pratices, *op. cit.*, p. 9 et p. 29.

« normes internationales,[…] la réglementation américaine, […] [le règlement de Google et […] la législation du pays demandeur »[155]. De janvier à juin 2017, les autorités françaises ont par exemple fait un total de 5661 demandes à la société Google, dont 12 demandes de divulgation d'urgence[156]. Google précise qu'il peut dans ce cadre fournir des informations sur l'utilisateur visé, mais ne précise pas s'il consent à fournir le contenu des communications[157].

1.4. Droits européen et paneuropéen international et européen

Tel que cela a déjà été mentionné, les dispositions de la **Convention sur la cybercriminalité** du Conseil de l'Europe[158] s'applique en France qui a ratifié celle-ci le 10 janvier 2006. Cette Convention est entrée en vigueur en France le 1er mai 2006.

De plus, la France a intégralement transposé la **directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale**[159] qui permet aux autorités de procédure pénale d'obtenir des preuves (documents, objets ou données) qui se trouvent dans un autre Etat. Les textes de transposition de cette directive sont la loi n° 2016-731 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (article 118)[160], et principalement l'ordonnance n° 2016-1636 du 1er décembre 2016[161] et son décret d'application du 7 avril 2017[162].

2. Réformes prévues

Il n'y a, à notre connaissance, **aucune réforme en cours** en France visant à modifier l'accès par les autorités de poursuite pénale françaises à des données stockées à l'étranger.
Les seules réformes susceptibles d'avoir un impact en France sont celles envisagées par l'Union européenne dans le cadre des **conclusions du Conseil pour l'amélioration de la justice pénale dans le cyberespace**, et par les **groupes créés en lien avec la Convention sur la cybercriminalité** (voir A., 2.).

---

155 La procédure en cas de demande de divulgation de données par une autorité étrangère à Google est détaillée dans les questions fréquentes, disponibles sous : https://support.google.com/transparencyreport/answer/7381738 (19.01.2018).

156 Ces chiffres sont disponibles sous : https://transparencyreport.google.com/user-data/overview?t=table&hl=fr&user_requests_report_period=series:requests,accounts;authority:FR&lu=user_requests_report_period (19.01.2018). Il peut être constaté que le plus grand nombre de demandes a été fait durant la période janvier-juin 2017. Lors de cette période, 63% des 5661 demandes ont été partiellement acceptées.

157 Google, Aide transparency report. Questions fréquentes sur l'acte de procédure relatif aux demandes de renseignements sur les utilisateurs, *op. cit.*, disponible sous : https://support.google.com/transparencyreport/answer/7381738 (25.01.2018).

158 Disponible sous : https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156d (15.01.2018)

159 Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, disponible sous : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32014L0041&from=DE (15.01.2018).

160 Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. L'article 118 de cette loi permet au gouvernement de prendre toute mesure nécessaire pour transposer la directive 2014/41/UE.

161 Ordonnance n° 2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale. Cette ordonnance a introduit les articles 694-15 à 694-50 dans le CPP concernant la décision d'enquête européenne en matière pénale. Aucune de ces dispositions ne traite du cas particulier de l'accès à des données stockées à l'étranger.

162 Décret n° 2017-511 du 7 avril 2017 relatif à la décision d'enquête européenne en matière pénale.

Malgré l'adoption de diverses lois en France venant renforcer la répression de la cybercriminalité, certains praticiens regrettent qu'aucune de celles-ci ne se soit attardée sur la **question des moyens d'investigation**, notamment en distinguant l'accès, la saisie et la copie de données informatiques des perquisitions, et en élargissant les possibilités d'accès à des données stockées à l'étranger ou sur les nuages (« clouds »)[163]. Cela permettrait de renforcer la lutte contre la cybercriminalité en offrant aux autorités de poursuite pénale davantage de moyens pour enquêter et rassembler des preuves relatives à des cyber-infractions ; ces infractions étant problématiques de ce point de vue dans la mesure où elles sont souvent commises à distance, parfois de l'étranger, par des auteurs anonymes et de façon instantanée.

Par ailleurs, un **groupe de contact permanent**, composé de grands opérateurs étrangers (Apple, Google, Twitter, Microsoft, Facebook) et des services du Ministère de la Justice et du Ministère de l'Intérieur français, s'est réuni à plusieurs reprises depuis sa création en 2015[164]. Deux objectifs sont assignés à ce groupe : l'amélioration du signalement et du retrait de contenus illicites par les opérateurs d'une part, et d'autre part une **meilleure prise en compte des demandes** d'obtention de données adressées par les enquêteurs français. Concernant ce second objectif, les travaux du groupe ont abouti à la mise en place de **formulaires de demandes harmonisés** et adaptés aux contraintes des opérateurs, améliorant ainsi la qualité et les délais de réponse.

3. Sanctions en cas d'accès direct par des autorités de poursuite pénale étrangères à des données stockées sur le territoire national

L'accès direct à des données constitue une **atteinte au secret des correspondances**, qui est punissable en droit français en vertu de l'article 432-9 du Code pénal lorsque cette atteinte est faite par des personnes dépositaires de l'autorité publique ou chargées d'une mission de service public[165], dont l'alinéa 2 concerne les correspondances électroniques :

> *« Est puni des mêmes peines [c'est-à-dire trois ans d'emprisonnement et 45 000 euros d'amende] le fait, par une personne visée à l'alinéa précédent [c'est-à-dire une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission] ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. ».*

Cette disposition permet également de **punir les agents d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications qui délivreraient le contenu des correspondances**, hors les cas prévus par la loi. On peut aisément en déduire que ces agents seraient punis s'ils délivraient le contenu à des autorités étrangères hors les cas prévus par la loi.

---

163 M. Robert, Cybercriminalité : les nouvelles réponses législatives, AJ pénal 2016, p. 412.

164 Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, État de la menace liée au numérique en 2017, janvier 2017, pp. 60-61, disponible sous : http://www.ladocumentationfrancaise.fr/rapports-publics/174000226/index.shtml (26.01.2018).

165 Cet article se trouve dans la section du Code pénal consacrée aux abus d'autorité commis contre les particuliers. De manière générale, les atteintes au secret des correspondances par toute personne privée sont sanctionnées par l'article 226-15 du Code pénal, al. 2 pour les correspondances électroniques.

Par contre, en ce qui concerne la **punissabilité des autorités étrangères**, au même titre que les autorités nationales françaises, en cas d'accès direct hors les cas prévus par la loi, l'hypothèse est plus périlleuse, car nous n'avons pu identifier aucune jurisprudence ou article de doctrine se prononçant sur cette question.

On peut seulement mettre cette question en parallèle avec le fait que, en règle générale, dans l'hypothèse où des **autorités étrangères se déplaceraient physiquement** hors de leur territoire dans le cadre d'une enquête, le principe de souveraineté des Etats empêche toute intervention d'agents étrangers sur le territoire national et confère aux agents nationaux une compétence exclusive d'exécution sur leur territoire[166]. L'interdiction d'exercice de la puissance étrangère en France a une valeur constitutionnelle en vertu de ce **principe de souveraineté nationale** énoncé dans la Constitution française. En effet, le Conseil constitutionnel a eu l'occasion de statuer sur l'accomplissement d'actes d'enquête sur le territoire national par une autorité étrangère, et ce dernier a considéré que cela portait atteinte aux conditions essentielles d'exercice de la souveraineté nationale[167].

G. IRLANDE

1. Access of criminal prosecution authorities to data stored abroad in electronic messages and on social networks

Although Irish law does not contain any provisions aimed specifically at access by law enforcement authorities in Ireland to social media data and emails stored in a foreign state, domestic legislation provides for indirect access to evidence, including such data, by way of **formal requests made to foreign law enforcement authorities under mutual legal assistance procedures.** These are contained in legislation known as the *Criminal Justice (Mutual Assistance) Act 2008* (the "MLA Act").[168]

However, it is understood that in practice, **direct cooperation between Irish law enforcement authorities and foreign-based internet service providers** represents a common route by which such data is obtained.[169] Non-content data[170] may be disclosed on a voluntary basis, according to the local laws of the country in which the data is stored and the internal policies of the service provider concerned. Disclosure of content data, however, usually requires a court order or equivalent, and in these circumstances, the MLA Act procedures may be relied on by Irish authorities to ensure that a

---

166 D. Rebut, Droit pénal international, *op. cit.*

167 Cons. const., 22 janvier 1999, n° 98-408 DC, considérant 38 : « Considérant, en revanche, qu'en application du 4 de l'article 99 du statut, le procureur [de la Cour pénale internationale] peut, en dehors même du cas où l'appareil judiciaire national est indisponible, procéder à certains actes d'enquête hors la présence des autorités de l'État requis et sur le territoire de ce dernier ; qu'il peut notamment recueillir des dépositions de témoins et " inspecter un site public ou un autre lieu public " ; qu'en l'absence de circonstances particulières, et alors même que ces mesures sont exclusives de toute contrainte, le pouvoir reconnu au procureur [de la Cour pénale internationale] de réaliser ces actes hors la présence des autorités judiciaires françaises compétentes est de nature à porter atteinte aux conditions essentielles d'exercice de la souveraineté nationale. »

168 The *Criminal Justice (Mutual Assistance) Act 2008*, available at http://www.irishstatutebook.ie/eli/2008/act/7/enacted/en/pdf (20.11.2017).

169 See Commission services, *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward,* May 22nd 2017, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (01.12.2017).

170 See section 3. of this country report for more information on the differences between "content" and "non-content" data.

formal request is made.[171] Where the assistance of foreign counterparts in a country covered by an agreement to which the MLA Act applies is needed to conduct a search for the evidence concerned, the Act sets out the procedures which Irish judicial or law enforcement authorities will need to follow.

The MLA Act **does not address the possibility of direct access** by Irish authorities to foreign-stored data. The extent to which direct requests for data stored abroad takes place is not revealed by the Irish Government.[172] It is understood, however, that in the absence of any legal basis for direct access to foreign-stored data, **requests** made by Irish authorities outside of the MLA Act procedures directly to foreign data controllers will be considered on a voluntary case-by-case basis in accordance with local laws.[173]

It should be noted that mutual legal assistance procedures under the MLA Act do not apply to requests for mutual assistance between member states of the European Union with regard to the **interception of telecommunications**.[174] Unlike mutual legal assistance procedures applying to access to stored evidence, the interception of telecommunications is addressed under separate rules set out in the MLA Act.[175]

The MLA Act is described as legislation to enable effect to be given in Ireland to certain international agreements, or provisions of such agreements between Ireland and other states relating to mutual assistance in criminal matters.[176] It sets out **procedures for Irish authorities to access evidence by way of cooperation with foreign authorities** and incorporates into Irish law a number of conventions, agreements and protocols which enable Ireland to provide mutual legal assistance to, and seek mutual legal assistance from, other countries with regard to the gathering of evidence more generally.

The principal purpose of the MLA Act, however, is to **establish a framework for formal requests for mutual legal assistance** between states covered by the international agreements referred to in the Act. It focuses principally on the steps foreign authorities must follow in order to secure mutual legal assistance from Ireland, but also contains provisions on how Irish authorities may proceed in seeking assistance from foreign law enforcement in securing evidence abroad.

---

171 See *infra* for more detail.

172 Requests are reported as being made: see Irish Examiner, *Gardai sought access to hundreds of private emails*, March 22nd 2013, available at http://www.irishexaminer.com/ireland/gardai-sought-access-to-hundreds-of-private-emails-226189.html (01.12.2017). It is however, understood that Ireland makes relatively few requests when compared to other EU States. See, for example, Microsoft, *Law Enforcement Requests Report,* 2017 (Jan-Jun) – Ireland, available at https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/ (20.12.2017). This reports that Ireland made 42 requests to Microsoft during the first half of 2017, compared to 3,312 by France and 3,875 by the UK during the same period.

173 For more detail about the treatment of such requests by social media companies in Ireland, see section 3. of this country report below. With regard to domestic requests, see for example, Digital Rights Ireland, *The Right to Privacy in Ireland – Stakeholder Report Universal Periodic Review, 25th Session – Ireland*, September 2015, available at https://www.digitalrights.ie/dri/wp-content/uploads/2015/12/Ireland_UPR-Stakeholder-Submission-DRI-and-Privacy-International_FINAL.pdf (19.12.2017).

174 Namely, third party access to messages in the process of being transmitted. See section 2 of this country report for more details.

175 MLA Act, *op. cit.,* section 8(2).

176 MLA Act, *op. cit.,* at (a) to Preamble to Act.

The **various conventions, agreements and frameworks** to which the legislation refers are set out in the Explanatory Notes to the MLA Act.[177] Ireland will give assistance to what are known as 'designated states'.[178]

A central provision of the MLA Act is that a **single point of contact, known as a Central Authority**, has the function of receiving, transmitting and otherwise dealing with requests in accordance with the relevant international instrument.[179] In Ireland, the **Central Authority is the Minister for Justice, Equality and Law Reform**.[180]

Responsibility for criminal investigations principally lies with *An Gardaí Síochána* (the Irish Police Service). **Formal requests to authorities in a designated state from *An Gardaí Síochána*** for assistance in obtaining evidence, including social media and emails, located in that jurisdiction must be processed via the Irish Central Authority in accordance with the MLA Act.[181]

We are informed that, in practice, the Irish Director of Public Prosecutions usually drafts requests for mutual legal assistance on behalf of *An Gardaí Síochána*, which are then sent via the Irish Central Authority directly to the 'appropriate' authority in the country where the evidence is held.[182] Such letter **must be sent to the Irish Central Authority for transmission to the appropriate authority**, or in urgent cases, directly to that authority.[183] An 'appropriate authority' is defined as a court or tribunal exercising criminal jurisdiction in the place in a designated state where the evidence referred to is to be obtained or any other body or authority recognized by the government of that state as the appropriate authority for receiving the letter.[184]

---

177 Explanatory Notes to the The *Criminal Justice (Mutual Assistance) Act 2008*, *ibid.* Further information on the operation of the Act is set out in a guide to the law and procedures published by Ireland's Department of Justice and Equality: *Mutual Legal Assistance in Criminal Matters – A Guide to Irish Law and Procedures,* undated, available at http://www.justice.ie/en/JELR/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf/Files/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf (20.11.2017).

178 These are:

- Member States of the European Union for the purposes of mutual assistance under the provisions of the EU Conventions/Protocol/Framework Decision;
- Iceland and Norway or any other designated state for the purposes of mutual assistance under the provisions of the EU Conventions/Protocol/Framework Decision;
- Any other state designated by the Minister for Foreign Affairs for the purposes of mutual assistance in accordance with the relevant international instrument.

(See Ireland's Department of Justice and Equality Department of Justice and Equality: *Mutual Legal Assistance in Criminal Matters – A Guide to Irish Law and Procedures, op. cit.*, p.7). Note that Ireland has signed but not ratified nor implemented the Council of Europe's *Convention on Cybercrime*, Treaty No. 185.

179 The MLA Act, *op. cit.,* section 8(2).

180 *Ibid*, section 8(1).

181 The MLA states that a judge may, in accordance with the relevant international instrument, issue a letter of request, asking for assistance in obtaining the evidence sought: section 73(1) MLA Act.

182 As described in email of 14.11.2017 of Shane O'Donovan, Information and Assessment Unit, Data Protection Commissioner for Ireland, in reply to email of the author. This would appear to be permitted under section 73(4) of the MLA Act, which states that where proceedings for an offence have been instituted or an offence is being investigated, the Director of Public Prosecutions may issue and transmit a letter of request directly to the appropriate foreign authority.

183 MLA Act, *op. cit.*, sections 73(1)-(3).

184 *Ibid*, sections 73(9)(a) and (b).

It should nevertheless be noted that the MLA Act does not concern requests by Irish law enforcement authorities for foreign-based evidence **where the assistance of the foreign authority is not required**. Information about the extent to which such direct requests are made or granted, however, is not made publicly available by Irish law enforcement authorities.[185]

2. Future reforms

It was announced in July 2016[186] by Ireland's Deputy Prime Minister that the Irish Government would be introducing legislation to tackle the loophole in existing legislation, which currently results in social media and internet communication services falling outside of the framework regulating the **interception of communications.**[187]

Currently, Part 3 of the MLA Act, contains specific provisions in relation to the interception – or surveillance - of telecommunications messages by Irish law enforcement authorities in accordance with domestic telecommunications legislation.[188] This Part is stated as only applying to requests for mutual assistance between member states of the European Union ("EU").[189] Unlike other requests for assistance in securing evidence, such as stored data, **requests for the interception of telecommunications messages are not routed via a Central Authority**.[190] Nevertheless, prior authorization is still required from the Minister for Justice, Equality and Law Reform in accordance with domestic legislation. According to the MLA Act, an approach to an EU Member State with the relevant authorisation must then be made to a "competent authority" in that State.[191]

However, it should be noted that it is currently accepted by the Irish government that domestic legislation on the interception of telecommunications does not apply to internet communications

---

185 Reported statistics in the media and as part of transparency reporting by companies such as Microsoft indicate that requests have been received from Irish law enforcement authorities, although it is not clear on what basis such requests have been made. See, for example, Microsoft, *Law Enforcement Requests Report,* 2017 (Jan-Jun) – Ireland, which reports that 42 requests were received from Irish law enforcement authorities in the first half of this year. Microsoft US claims that as a minimum, it will require a signed document issued pursuant to local law and rules, such as a subpoena or equivalent before disclosing non-content data, and a warrant or court order with regard to content data.

186 See The Irish Times, *Garda to get power to intercept texts, emails and social media*, 6 July 2016, available at https://www.irishtimes.com/news/politics/garda-to-get-power-to-intercept-texts-emails-and-social-media-1.2711618 (04.12.2017).

187 "Interception" has been defined as follows: "*A person intercepts a communication in the course of its transmission if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication."* See A. Hale and J. Edwards, *Getting it Taped*, (2006) 12 Computer and Communications Law Review 71.

188 Such as the *Postal and Telecommunications Services Act 1983*, available at http://www.irishstatutebook.ie/eli/1983/act/24/enacted/en/html (01.12.2017) and the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, available at http://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/html (01.12.2017).

189 See Ireland's Department of Justice and Equality: *Mutual Legal Assistance in Criminal Matters – A Guide to Irish Law and Procedures, op. cit.*, p. 17.

190 MLA Act, *op. cit.*, section 8(2).

191 It should be also be noted that, broadly speaking, in all cases of interception as between EU member states, where Ireland or a member state cannot directly intercept telecommunications messages, telecommunications providers can be obliged to facilitate interception of the messages where a lawful warrant or order for interception has been made: see MLA Act, *op. cit.*, section 28.

services.[192] Such entities are not considered as regulated "licensed operators" or "authorized undertakings" in the same way as telecoms companies such as landline, cable and mobile phone providers and fixed and mobile internet service providers.

Accordingly, although there is no formal power for Irish law enforcement authorities to intercept internet communications, it is claimed that there is, equally, no effective statutory regulation of the manner in which Irish law enforcement authorities may carry out such surveillance.[193] Given the reliance of the MLA Act on domestic legislation as the basis for the interception of communications by Irish authorities, there is arguably no current legal obstacle to direct surveillance of internet communications by Irish law enforcement authorities both at home and abroad. This "lacuna" in the law is the subject of the proposed reforms.

It is understood that, as of 23 November 2017, the proposed legislation has not yet been finalized.[194]

Under the revised legislation, the **regime governing the powers of the Irish Police to intercept post and telephone communications will be extended** to other more modern forms of communication and companies providing these services. Police will be provided with legislative authority to intercept such communications, but will need to do so in accordance with rules and procedures set out under existing telecommunications legislation, namely, the *Interception of Postal Packets and Telecommunications (Regulation) Act 1993* and the *Postal and Telecommunications Services Act 1983*.[195]

Telecommunications companies which may be required by the Minister for Communications to comply with the lawful interception framework will, under the proposals, include "Information Society Services".[196] The policy document of the Department of Justice and Equality states that:

> *"The Department is of the view that this definition will cover internet referencing services and social media."*[197]

Corresponding amendments to Part 3 of the MLA Act are stated as being technical in nature and relating primarily to the updated terminology in the amended telecommunications legislation.[198]

---

192 See Department of Justice and Equality, *Policy Document – Amendments to the legislative basis for the lawful interception of communications*, undated, available at http://www.justice.ie/en/JELR/Amendments_to_the_legislative_basis_for_the_lawful_interception_of_communications_policy_paper.pdf/Files/Amendments_to_the_legislative_basis_for_the_lawful_interception_of_communications_policy_paper.pdf (01.12.2017), chapter 6.

193 See Digital Rights Ireland, *The Right to Privacy in Ireland – Stakeholder Report Universal Periodic Review, 25th Session – Ireland*, September 2015, *op. cit.*

194 See answer to Parliamentary question from Deputy Eamon Ryan to Minister for Justice and Equality, on 23.11.2017, available at http://www.justice.ie/en/JELR/Pages/PQ-23-11-2017-113 (04.12.2017).

195 *Op. cit.*

196 As defined by EC Directive 98/34/EC.

197 Department of Justice and Equality, *Policy Document – Amendments to the legislative basis for the lawful interception of communications,* undated (but thought to be 22.11.2016), Chapter 6 (no page numbering) under title "*Amendments to Section 110 of the Postal and Telecommunications Services Act 1983*", available at http://www.justice.ie/en/JELR/Amendments_to_the_legislative_basis_for_the_lawful_interception_of_communications_policy_paper.pdf/Files/Amendments_to_the_legislative_basis_for_the_lawful_interception_of_communications_policy_paper.pdf (04.12.2017).

198 Department of Justice and Equality, *Policy Document – Amendments to the legislative basis for the lawful interception of communications*, *op. cit.* Accordingly, this will have no impact on stored data forming the object of mutual legal assistance procedures covered by other parts of the MLA Act.

There are **no other known amendments proposed** in relation to the MLA Act or the legal framework more generally.

3. National law sanctions against direct access by a foreign criminal prosecution authority to data stored on the national territory in electronic messages or on social networks

The MLA Act sets out the conditions under which the Irish Central Authority may deal with requests from foreign authorities for assistance from Irish law enforcement authorities in obtaining evidence for criminal investigation proceedings in a foreign state.[199] The Act, however, **does not contain general enforcement mechanisms based on criminal or civil liability**. Instead, it is understood that the consequence of failing to meet the conditions of a valid request is simply that the request for assistance is denied. It is not known whether individual arrangements with regard to liability may be made as part of international or bilateral agreements on mutual legal assistance, but these are in any event beyond the scope of this enquiry.

There are otherwise **no known legislative provisions or other rules aimed specifically at the liability of foreign criminal prosecution authorities** in the case of unlawful direct access to electronic messages or social network data.[200]

It should be noted that direct access by foreign criminal prosecution authorities to social media data stored in Ireland is reported as taking place pursuant to requests to Irish-based social media companies such as Microsoft Ireland and Facebook Ireland. Although there is no known specific legal basis for requests to be made to data controllers for such data, **Irish data protection law effectively permits the voluntary disclosure of stored data and communications** in certain circumstances. Under section 8(b) of the *Data Protection Acts 1988 and 2003* (the "Data Protection Acts"),[201] an exemption is provided to data controllers with regard to the restrictions on data processing laid down in the Data Protection Acts. This 'law enforcement' exemption applies if the processing is, among other things, "*required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders….*"[202] This approach to dealing with requests received directly from foreign law enforcement authorities is, in principle, endorsed by the Data Protection Commissioner of Ireland.[203]

---

199 See MLA Act, *op. cit.,* section 75.

200 With regard to the interception of communications, section 98 of the *Postal and Telecommunications Services Act 1983* makes it an offence for a person, among other things, to unlawfully intercept telecommunications messages. As a general provision however, it is not clear to what extent this can or would be relied on in relation to foreign law enforcement authorities.

201 *Data Protection Act 1988,* number 25 of 1988, and *Data Protection Act 2003,* number 6 of 2003, revised, updated to 14 October 2014; consolidated version available at https://www.dataprotection.ie/docs/DATA-PROTECTION-ACT-1988-REVISED-Updated-to-14-October-2014/1469.htm (21.11.2017).

202 See, for example, Facebook Ireland Ltd, contained at Appendix 5 of Data Protection Commissioner, *Facebook Ireland Ltd – Report of Audit*, 21 December 2011, available at https://www.dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf (21.11.2017). For the purposes of this country report, the classification of data requests as made by Facebook Ireland's Privacy Policy is adopted here.

203 See Data Protection Commissioner, *Facebook Ireland Ltd – Report of Re-Audit,* 21 September 2012, available at https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf (01.12.2017), pp. 34-35. This includes a sample of requests from foreign law enforcement authorities examined by the Data Protection Commissioner.

How such law enforcement requests are dealt with by a social media company, as data controller, appears to depend on the type of data requested. A distinction is to be made between, first, **non-content data** (such as basic subscriber information and logs of IP addresses) and, secondly, **user-generated content data** (such as messages, photos and videos). A third category is that of **emergency requests** for disclosure of user data.

With regard to requests **for non-content data**, a data controller has discretion to determine whether the law enforcement exemption applies.[204] In effect, it allows for voluntary disclosure subject to consideration on a case-by-case basis. For example, Facebook Ireland, as a data controller, systematically assesses, in examining this question, the legal basis for compatibility with applicable local law of the requesting state and the legal authority of the requesting law enforcement agency.[205]

Insofar as **content data** is concerned, it is understood that data controllers such as Facebook Ireland[206] and Microsoft Ireland[207] will not provide such information without being legally compelled to do so under the terms of a warrant or other statutory power of compulsion under Irish law. In taking this approach, a data controller is able to rely on section 8(e) of the Data Protection Acts, which exempts processing which is, "*required by or under any enactment or by a rule of law or order of a court*." Any processing of data in compliance with such a requirement will fall outside of the usual restrictive rules under the Data Protection Acts.

In practice, this means that any non-Irish search warrant for content data will only be complied with if it is enforceable as a matter of Irish law.[208] In other words, **any request for a search for evidence from a designated foreign state will need to be "domesticated"**.

Accordingly, the consequence of a foreign law enforcement authorities failing to comply with these conditions is simply that **the relevant request will be denied**.

Finally, **disclosure to law enforcement authorities in emergencies** is permissible in light of section 8(d) of the Data Protection Acts which exempts from usual data processing rules any processing which is, "*required urgently to prevent injury or other damage to the health of a person or serious loss of or*

---

204 This is not the case for domestic access to communications data by the Ireland for use within Ireland, pursuant to the *Communications (Retention of Data) Act 2011* (available at http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html (21.11.2017)). This Act only applies to serious offences and section 7 places a mandatory requirement on data controllers to provide the data. According to section 2 of the Act, the content of communications is not covered in disclosure requests. See also Irish Human Rights and Equality Commission, *Memorandum: to Justice John L. Murray – Review of the Law on Access to Communication Data*, 13 June 2016, available at https://www.ihrec.ie/app/uploads/2016/11/Memorandum_Review-of-the-Law-of-Access-to-Communication-Data.pdf (21.11.2017), p.14.

205 See *Facebook Ireland Ltd – Report of Audit*, 21 December 2011, available at https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf (21.11.2017), pp.98-99.

206 Facebook Ireland is quoted as saying, "*should the law enforcement agency require content information from Facebook Ireland, we will require that we be served with a legally compelling request under Irish law. The Gardaí (Irish Police) will be required to produce a search warrant or similar coercive document. Non-Irish search warrants will only be respected by Facebook Ireland if they are enforceable as a matter of Irish law. This will require that any such orders be domesticated by way of application to the Department of Justice pursuant to the Criminal Justice (Mutual Assistance) Act 2008*." See *ibid,* p. 99.

207 See background to the case of *Microsoft Corp. v. United States*, 829 F.3d 197 (2nd Cir. 2016).

208 See the example of Facebook at *Facebook Ireland Ltd – Report of Audit*, 21 December 2011, *op. cit.,* at Appendix 5, p. 218.

damage to property." In light of the MLA Act,[209] it is understood that a request from a foreign authority must still be directed, in the first instance, to the Irish Central Authority.

The Constitution of Ireland does not explicitly guarantee a right to privacy, but courts have recognized an un-formulated **right to privacy** as one of the personal rights in the Constitution.[210] The statutory right to data protection is set out **under the Data Protection Acts.**[211] **This legislation sets out various offences**, but these are **aimed rather at data controllers and data processors** who provide unauthorized access to personal data.[212]

H. ITALIE

1. Accesso da parte dell'autorità giudiziaria a dati informatici conservati all'estero e contenuti in messaggi elettronici e reti sociali

1.1. Quadro normativo generale

La Convenzione di Budapest è stata ratificata dall'Italia con la legge 18 marzo 2008 n. 48, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"[213].

L'art. 234 bis del codice di procedura penale prevede il **consenso del "legittimo titolare"** per l'acquisizione di documenti e dati informatici **conservati all'estero**[214].

> *Art. 234-bis. Acquisizione di documenti e dati informatici. 1. È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare.*

Il **dovere di fornire i dati informatici è previsto da diverse norme**, che disegnano una disciplina composita e non sempre di agevole coordinazione. In primo luogo va menzionato l'art. 256 del codice di procedura penale italiano, come modificato dall' art. 8, comma 6, della legge di ratifica della convenzione di Budapest, che prescrive **il dovere di esibizione di segreti, includendo tra questi anche "i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto**". L'inottemperanza all'ordine è sanzionata dall'art. 650 del codice penale che prevede

---

209 In particular, section 6.

210 *McGee v. Attorney General* [1974] Irish Reports 284; *Kennedy and Arnold v. Attorney General* [1987] Irish Reports 587.

211 *Op. cit.*

212 One provision based on the liability of someone other than a data controller or data processor is that making it an offence for any person who is not a data controller or data processor to obtain unauthorized access to personal information and to then disclose it to others. Direct access by a foreign criminal prosecution authority may potentially fall into this category. There are however, no examples of which we are aware, of such a body being held liable under Irish data protection law in circumstances where personal data has been directly accessed without prior authorization: see Data Protection Acts, *op. cit*., section 22.

213 Suppl. ordinario n. 79 alla Gazz. Uff., 4 aprile, n. 80 (www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48!vig= (9.1.2017).

214 Cf. l'art. 2, comma 1-bis, D.L. 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla L. 17 aprile 2015, n. 43. Il "QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace" afferma che i fornitori di servizi aventi la propria sede all'estero rispondono alle richieste di informazioni in base agli articoli sopra citati su base volontaria.

l'arresto fino a 3 mesi e un'ammenda massima di 206 euro ma la norma non si applica ai fornitori avente sede all'estero perché la disciplina dei reati commessi all'estero da stranieri non include i c.d. reati minori.

Il dovere di fornire dati informatici è inoltre previsto dall'art. 96 comma 1 del d.lgs. 259/2003 (codice delle comunicazioni elettroniche) come modificato dalla legge 23 giugno 2017, n. 103 (in G.U. 04/07/2017, n.154)[215].

L'art. 132bis del d.lgs. 196/2003 (Codice di protezione dei dati personali) prevede che i fornitori istituiscano procedure interne per corrispondere alle richieste di accesso dati effettuate dalle autorità[216]. L'art. 5 d.lgs. n. 196/2003 prevede esplicitamente la sua applicazione extraterritoriale.[217]

---

215 «Art. 96 (Prestazioni obbligatorie) 1. Le prestazioni a fini di giustizia effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie sono obbligatorie per gli operatori; i tempi ed i modi sono concordati con le predette autorità fino all'approvazione del decreto di cui al comma 2. / 2. (un) decreto del Ministro della giustizia e del Ministro dello sviluppo economico, di concerto con il Ministro dell'economia e delle finanze, da emanare entro il 31 dicembre 2017 (…) individua i soggetti tenuti alle prestazioni obbligatorie di intercettazione, anche tra i fornitori di servizi, le cui infrastrutture consentono l'accesso alla rete o la distribuzione dei contenuti informativi o comunicativi, e coloro che a qualunque titolo forniscono servizi di comunicazione elettronica o applicazioni, anche se utilizzabili attraverso reti di accesso o trasporto non proprie; c) definisce gli obblighi dei soggetti tenuti alle prestazioni obbligatorie e le modalità di esecuzione delle stesse, tra cui l'osservanza di procedure informatiche omogenee nella trasmissione e gestione delle comunicazioni di natura amministrativa, anche con riguardo alle fasi preliminari al pagamento delle medesime prestazioni. 3. In caso di inosservanza degli obblighi contenuti nel decreto di cui al comma 2, si applica l'articolo 32, commi 2, 3, 4, 5 e 6. 4. Fino all'emanazione del decreto di cui al comma 2 il rilascio di informazioni relative al traffico telefonico e' effettuato in forma gratuita. In relazione alle prestazioni a fini di giustizia diverse da quelle di cui al primo periodo continua ad applicarsi il listino adottato con decreto del Ministro delle comunicazioni del 26 aprile 2001, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 104 del 7 maggio 2001. 5. Ai fini dell'erogazione delle prestazioni di cui al comma 2 gli operatori hanno l'obbligo di negoziare tra loro le modalità di interconnessione allo scopo di garantire la fornitura e l'interoperabilità delle prestazioni stesse. Il Ministero può intervenire se necessario di propria iniziativa ovvero, in mancanza di accordo tra gli operatori, su richiesta di uno di essi.».

216 "Art. 132-bis Procedure istituite dai fornitori 1. I fornitori istituiscono procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni che prevedono forme di accesso a dati personali degli utenti. 2. A richiesta, i fornitori forniscono al Garante, per i profili di competenza, informazioni sulle procedure di cui al comma 1, sul numero di richieste ricevute, sui motivi legali addotti e sulle risposte date".

217 Questo significa che il Garante per la protezione dei dati personali può adottare provvedimenti sanzionatori anche nei confronti di fornitori esteri che non rispettano le regole italiane anche quando i dati sono conservati all'estero. Tuttavia, si tratta di provvedimenti sanzionatori tutti volti a rendere la condotta del fornitore di servizi conforme al codice italiano di trattamento dei dati personali e non già a sanzionare l'inosservanza dell'obbligo di fornire dati alle autorità (il garante non ha il potere di ordinare l'esibizione delle informazioni richieste ai sensi del già citato art. 132, potere riservato all'autorità di polizia e giudiziaria).

1.2. L'ordine europeo di indagine penale e la convenzione di mutua assistenza penale (MAP)

All'art. 256 c.p.p. rinviano gli artt. 25 e 45 del decreto legislativo che ha trasposto la direttiva 2014/41/UE.[218]

Il decreto introduce una disciplina specifica per l'ordine di indagine penale emesso dalla **"autorità competente di uno Stato membro dell'Unione"** e rivolto alla "autorità competente di un (altro) Stato membro dell'Unione" che dovrà ricevere, riconoscere e dare esecuzione ad esso."

> ***Art. 25.*** *Richieste di documentazione inerente alle telecomunicazioni*
>
> *1. Il procuratore della Repubblica dà esecuzione all'ordine di indagine finalizzato all'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche con le forme e le modalità dell'articolo 256 del codice di procedura penale.*
>
> ***Art. 45.*** *Richiesta di documentazione inerente alle telecomunicazioni*
>
> *1. Il pubblico ministero o il giudice che procede possono trasmettere all'autorità di esecuzione ordine di indagine al fine di ottenere i dati esterni relativi al traffico telefonico o telematico nonché l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni.*
>
> *2. L'ordine di indagine contiene i dati tecnici necessari all'individuazione dell'utenza o del sistema informatico, ogni informazione utile ai fini dell'identificazione della persona che li ha in uso e dell'operatore, se noti, nonche' l'indicazione del reato per il quale si procede.*

Non è semplice comprendere che cosa si intenda per **"dati esterni".** Dalle risposte che le autorità italiane hanno dato al questionario della commissione[219], pare che i dati che possono essere richiesti direttamente al "service provider" siano i soli dati necessari all'identificazione dell'utente, ossia i c.d. "subscriber data". Tuttavia, come precisa lo stesso rapporto, non c'è una prassi consolidata, né statistiche disponibili. Le richieste di dati sono fatte direttamente attraverso il portale del detentore dei dati. Si può inoltre aggiungere che la formulazione dell'articolo è ampia e che l'espressione "dati esterni relativi al traffico telefonico o telematico nonché l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni" potrebbe essere interpretata come idonea a includere qualsiasi tipo di dato informatico.

Il D. Lgs. 5 aprile 2017, n. 52 che ha attuato la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (Bruxelles, 29 maggio 2000) [220], prevede lo "**scambio spontaneo di informazioni"** tra autorità giudiziarie (art. 9)[221].

---

218 G.U., 13 luglio 2017, n. 162: www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017-06-21;108!vig= (9.1.2017).

219 Sopra, nota 195.

220 GU 27 aprile 2017, n. 97: www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017-04-05;52!vig=

221 Cf. l'Art. 9 (Scambio spontaneo di informazioni): 1. E' consentito, nell'ambito di un procedimento penale o di un procedimento amministrativo, lo scambio diretto e spontaneo di informazioni utili e di atti con l'autorità competente di altro Stato Parte. 2. Le informazioni e gli atti ricevuti sono utilizzabili nel rispetto dei limiti indicati dall'autorità competente dello Stato Parte. Il decreto prevede inoltre: l'utilizzo della posta elettronica certificata, oltre alla posta ordinaria, per le notificazioni (art. 5); la trasmissione diretta di richieste di assistenza giudiziaria, con l'eccezione delle richieste dirette in Gran Bretagna e Regno Unito, per le quali è d'obbligo sollecitare il Ministero della Giustizia (art. 7); l'esecuzione della richiesta di assistenza di uno Stato Parte per attivita' probatoria nelle forme dello stato richiedente, sempre che non siano contrarie all'ordine pubblico internazionale interno (art. 8, spec. comma 4). L'art. 23 prevede inoltre una procedura specifica per l'intercettazione di dati conservati all'estero che si fonda sulla

1.3. Prassi

1.3.1. Assenza di formalismo

Nella pratica, la richiesta dei dati in possesso del fornitore di servizi informatici che ha sede all'estero non è effettuata con procedure particolari, non si fa una distinzione tra ordini da eseguirsi in Italia e ordini da eseguirsi all'estero, né tra ordini richiesti dall'autorità italiana e estera. Inoltre, la richiesta può essere indirizzata alla sede legale del fornitore di servizio ma anche semplicemente ad un indirizzo elettronico, che come tale, non è situato in un luogo fisico[222].

Ciò che rileva è che il soggetto richiesto sia effettivamente in grado di eseguire l'ordine di esibizione dei dati richiesto dall'autorità. Questa modalità è oggetto di accordi che lo Stato italiano ha concluso con i seguenti fornitori di servizi: facebook, twitter, Ask, Google, Microsoft e skype[223].

Al fornitore di servizi (facebook, instagram, google etc.) è notificato un "decreto di acquisizione files di log" che si basa sull'art. 256 c.p.p.

In informatica, il termine "file di log" indica qualsiasi attività effettuata dall'utente mediante un computer. Si precisa, tuttavia, che gli accordi conclusi con i fornitori di servizi elencati sopra prevedono unicamente che siano fornite informazioni relativamente a "subscriber data and IP connections"[224].

Si evince dal questionario sopra citato, sia pure nell'assenza di statistiche adeguate, le sole richieste effettuate attraverso canali di mutua assistenza (dunque non direttamente al service provider) sembrano essere quelle dirette oltre oceano: the "Directorate General for Criminal Affairs, Office II" only sent requests to Canada and the US. A search carried out on the period from 1 January 2000 to 11 May 2016 revealed that 263 requests for legal assistance were sent to the US, 140 of which contained requests for acquiring computerized data processed and stored by Providers located on the territory of the United States of America".

---

cooperazione internazionale. Regole simili sono previste per l'acquisizione mediante ordine all'operatore di rete situato nel territorio italiano e per l'intercettazione disposta da un'autorità estera nel territorio italiano.

222 Questa conclusione trova conferma nella risposta che le autorità italiane hanno dato al "QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace": *Currently, there's not mandatory direct cooperation between Law Enforcement and third parties service providers (telecommunications and cloud). Requests could be made under law regulation and through specific court order (except basis data such as account subscriber, registration forms*) ". E, più avanti nello stesso documento: "*Prosecutors can make requests independently from any LE cooperation channels".* Si veda ancora la risposta alla domanda*: "5. Do authorities from your Member State make direct requests to service providers in another EU Member State or in third countries?*" La risposta fornita dale autorità italiane è "*Yes, both in EU Member States and third countries".* Lo stesso documento precisa che: " *The requests are made in electronic form, but are not tracked and there is not a central repository*" e che "*currently there's no standard practices and no statistics available, also considering that in most cases the requests are submitted through (directly) a portal provided by the owning companies*".

223 "QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace".

224 *Ibidem.*

1.3.2. Uso di captatori informatici (malware)

Un'altra modalità, molto controversa, di acquisizione dei file di log riguarda il loro prelievo diretto, in particolare tramite malware. Questo può avvenire sia attraverso l'intercettazione di comunicazioni, compresi i messaggi di posta elettronica, conservati nelle caselle di posta in entrata e in uscita, sia tramite accesso diretto al computer, sia tramite inserimento di un programma spia[225], o con estrapolazione di dati contenuti nella memoria del "personal computer"[226], ad esempio tramite perquisizione e sequestro[227]. Vale la pena di precisare, a questo proposito, che "il sequestro probatorio di un sistema informatico (personal computer) che determini, in mancanza di una specifica motivazione, un'indiscriminata apprensione di tutte le informazioni in esso contenute è illegittimo".[228]

> *"Le intercettazioni vengono effettuate mediante un software, del tipo definito simbolicamente trojan horse, che è chiamato, nelle prime sentenze che si sono confrontate con esso "captatore Informatico" (Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Virruso, Rv. 246954) o "agente intrusore" (Sez. 6, n. 27100 del 26/05/2015, Musumeci, Rv. 265654).."*[229]

Si occupano di intercettazioni tramite "captatore informatico" sia il Decreto legge 18 febbraio 2015, n. 7, (Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché' proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione)[230]; sia il Decreto legislativo 29 dicembre 2017, n. 216 (Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103[231], che entra in vigore il 26 gennaio 2018.

La giurisprudenza ha elaborato una serie di principi in occasione di prove acquisite tramite intercettazioni[232].

1. Le intercettazioni di comunicazioni se eseguita, almeno all'inizio o in parte, su territorio italiano, non necessita di rogatoria per il solo fatto che le comunicazioni siano avvenute all'estero[233].
2. Viceversa la rogatoria è indispensabile se le comunicazioni o le conversazioni avvengono interamente all'estero e sono captate esclusivamente da un gestore straniero[234].

---

225 Sez. 4, n. 40903 del 28/06/2016, Grassi e altri.

226 Sez. 6, n. 27100 del 26/05/2015, Musumeci.

227 Sez. 5, n. 16556 del 14/10/2009 - dep. 2010, Virruso, Rv. 246954.

228 Cass. VI, n. 24617/2015. V. già Molinari, Questioni in tema di perquisizione e sequestro di materiale informatico, in Cass. pen. n. 2/2012.

229 Cassazione penale, sez. un., 28/04/2016, (ud. 28/04/2016, dep.01/07/2016), n. 26889.

230 GU n.41 del 19-2-2015.

231 GU Serie Generale n.8 del 11-01-2018.

232 Cf. Dati ricavati attraverso il Codice penale commentato contenuto nella banca dati "IUSEXPLORER".

233 Cass. IV, n. 8588/2008 in un caso di intercettazione tramite microspia collocata in un'auto che, partita dall'Italia, ha transitato all'estero. Idem per la "procedura di istradamento", ossia il convogliamento delle chiamate in partenza dall'estero in un nodo sito in Italia (Cass. V, 2 luglio1998, Assisi; Cass. IV, n. 32924/2004; Cass. IV, n. 37646/2004; Cass. VI, n. 7258/2005; Cass. VI, n. 10051/2008; Cass. I, n. 13972/2009; Cass. VI, n. 7634/2015).

234 Cass. IV, n. 9161/2015; Cass. III, n. 25833/2016.

3. I messaggi scambiati attraverso un sistema Blackberry, acquisiti con la collaborazione del produttore del sistema operativo avente sede all'estero e senza previo ricorso a rogatoria internazionale, sono utilizzabili nel processo italiano[235].

2. Legislazione recente e progetti di riforma

La legislazione recente e i progetti di riforma adottati dal Parlamento italiano sono frutto della necessità di adeguare la legislazione italiana a quella europea. Abbiamo già menzionato il d. lgs. del 5 aprile 2017 n. 52 che ha dato attuazione alla Convenzione di mutua assistenza tra gli Stati membri dell'Unione europea, firmata a Bruxelles il 29 maggio 2000 (di seguito indicata come MAP). La direttiva europea 2014/41/UE è stata trasposta in Italia con il decreto legislativo 21 giugno 2017, n. 108, rubricato "Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale"[236]. La direttiva intende semplificare la disciplina previgente, alquanto complessa, prevedendo esplicitamente la prevalenza degli atti normativi adottati in forza di essa su eventuali norme difformi.[237]

Secondo quanto indicato dal Ministero della Giustizia italiano (circolare del 26 ottobre 2017, n.150574, denominata "manuale operativo")[238] è stata notificata alla Commissione UE insieme al decreto di recepimento, una dichiarazione a mente della quale l'Italia continuerà ad applicare gli Accordi aggiuntivi alla Convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959 stipulati con l'Austria (Vienna, 20.2.1973) e la Germania (Roma, 24.10.1979)[239]. Questi accordi prevedono procedure di assistenza più fluide e la possibilità di trasmettere la richiesta di assistenza nella lingua del paese richiedente in luogo di quella del paese di esecuzione. La circolare chiarisce inoltre come trattare richieste difformi.

Il decreto legislativo 3 ottobre 2017, n. 149 modifica il Libro XI del codice di procedura penale, nuovo Titolo I-bis, specificamente dedicato ai Principi generali del mutuo riconoscimento delle decisioni e dei provvedimenti giudiziari tra Stati membri dell'Unione europea, introducendo l'art. 696-quinquies (Limiti al sindacato delle decisioni giudiziarie degli altri Stati membri):

---

235 l'attività di intercettazione del traffico telematico cd. "PIN to PIN", svolta secondo le modalità di cui all'art. 266 bis cod. proc. pen., relativa a comunicazioni registrate da terminale sito sul territorio italiano, rispetto alle quali la società canadese di gestione del traffico si era limitata a comunicare i dati in suo possesso che identificavano i possessori dei nickname associati ai codici PIN monitorati (Cass. IV, n. 16670/2016)

236 *Supra.*

237 L'art. 34 della direttiva prevede che essa prevalga in caso di contrasto con le corrispondenti regole contenute in strumenti normativi precedenti: la Convenzione europea di assistenza giudiziaria in materia penale adottata dal Consiglio d'Europa il 20 aprile 1959, con i relativi protocolli addizionali e con gli accordi bilaterali stipulati a norma dell'articolo 26 della Convenzione; b. la Convenzione di applicazione dell'accordo di Schengen, ratificata dall'Italia con legge 30 settembre 1993, n. 388; la Convenzione di Bruxelles del 29 maggio 2000 sull'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (M.A.P.), recentemente attuata con il D. lgs. 5 aprile 2017, n. 52, che entrerà in vigore quando saranno decorsi novanta giorni dalla notifica al Segretariato generale del Consiglio dell'Unione europea ; d. la Decisione quadro 2003/577/GAI relativa all'esecuzione dei provvedimenti di blocco dei beni o di sequestro probatorio, attuata nel nostro ordinamento con d. lgs. 15 febbraio 2016, n. 35, entrato in vigore il 26 marzo 2016 ; la Decisione quadro 2008/978/GAI in tema di mandato europeo di ricerca delle prove (M.E.R.), mai trasposta nel nostro ordinamento (5) e comunque abrogata, prima della scadenza del termine di trasposizione della Direttiva OEI, dal Regolamento 95/2016 del Parlamento europeo e del Consiglio del 20 gennaio 2016.

238 https://giustizia.it/giustizia/it/mg_1_8_1.page;jsessionid=RuEfUcjO1DlIAFLWAyYlSfEB?facetNode_1=1_1(2017)&contentId=SDC58426&previsiousPage=mg_1_8 (26.1.2018).

239 *Ibidem*.

"L'autorità giudiziaria riconosce ed esegue le decisioni e i provvedimenti giudiziari degli altri Stati membri senza sindacarne le ragioni di merito, salvo che sia altrimenti previsto. È in ogni caso assicurato il rispetto dei principi fondamentali dell'ordinamento giuridico dello Stato". Coerente è la previsione dell'art. 696-novies (Impugnazioni) per la quale non è ammessa l'impugnazione delle decisioni sul riconoscimento e l'esecuzione di un provvedimento emesso dall'autorità giudiziaria di uno Stato membro "per motivi di merito, salvo quanto previsto dall'articolo 696-quinquies".

3. Sanzioni previste per l'accesso abusivo a sistemi informatici

L'art. 615 ter e l'art 615 quater c.p., puniscono l'accesso abusivo a un sistema informatico e la detenzione e diffusione abusiva di codici di accesso a sistemi informatici, che non opera . nessuna distinzione tra accesso ai dati effettuato da cittadini italiani residenti in Italia o stranieri residenti all'estero[240].

In dottrina, a questo proposito, si parla di "domicilio informatico" per indicare che si tratta di un luogo privato, che implica lo *ius excludendi* e la cui violazione è penalmente sanzionata, salvo che vi siano cause di esonero della responsabilità.

Una di queste è sicuramente data dalla necessità investigative.

Anche in questo caso, tuttavia, "Integra il delitto previsto dall'art. 615-ter, comma 2, n. 1, c.p., la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso (nella specie, Registro delle notizie di reato: Re. Ge.), acceda o si mantenga nel sistema per regioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita"[241].

---

240 Art. 615 ter: (1) Chiunque abusivamente si introduce in un sistema informatico o telematico (2) protetto da misure di sicurezza (3) ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio. At. 615 quater: Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo (2), è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro. La pena è della reclusione da uno a due anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater.

241 Cass. S.U., n. 41210/2017.

I reati per i quali è possibile l'accesso a sistemi informatici sono indicati dall'art. 266 c.p.p., al quale l'art. 266 bis[242] rinvia[243].

IV. RÉSUMÉ COMPARATIF

1. Accès direct

En matière d'accès direct à des communications électroniques stockées à l'étranger, **deux catégories peuvent être distingués** : celle comprenant les Etats dont le droit national ne permet pas à ses autorités de poursuite pénale d'exiger l'accès direct à des données privées qu'elles savent stockées à l'étranger (Allemagne, Autriche, France, Irlande et Italie) (1.1.), et celle comprenant la Belgique qui au contraire prévoit cette possibilité dans sa législation nationale (1.2.). Les Etats-Unis sont actuellement dans l'attente d'une décision de la Cour suprême voire d'un changement législatif qui devrait permettre de déterminer à laquelle de ces deux catégories ils correspondent (1.3.).

1.1. Accès direct et bonne volonté des fournisseurs

1.1.1. Accès direct via les fournisseurs

Les droits nationaux **allemand, autrichien, français, irlandais et italien** ne prévoient pas la possibilité, pour leurs **autorités de poursuite pénale respectives, de pouvoir obliger les fournisseurs à leur donner accès directement à des données stockées à l'étranger** dans des messageries électroniques et sur des réseaux sociaux.

Leurs autorités de poursuite pénale doivent, pour ce faire, avoir recours aux procédures d'**entraide judiciaire internationale**.

Néanmoins, on observe que **des demandes d'accès direct auprès des fournisseurs** étrangers / pour le contenu hébergé à l'**étranger ont lieu** même si elles sont subordonnées à la bonne volonté et aux obligations des fournisseurs en vertu du droit des pays où ils se trouvent.

---

242 Art. 266 bis. "1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi".

243 Si tratta dei seguenti: 1. L'intercettazione di conversazioni o comunicazioni telefoniche [295] e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati: a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4; b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4; c) delitti concernenti sostanze stupefacenti o psicotrope; d) delitti concernenti le armi e le sostanze esplosive; e) delitti di contrabbando; f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono; f-bis) delitti previsti dall'articolo 600-ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1 del medesimo codice, nonché dall'art. 609-undecies; f-ter) delitti previsti dagli articoli 444, 473, 474, 515, 516 e 517-quater del codice penale.f-quater) delitto previsto dall'articolo 612-bis del codice penale. 2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che puo' essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa [615-bis c.p.]. 2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile e' sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater.

1.1.2. Accès direct aux communications par les autorités

Dans les cas où il n'est pas nécessaire d'avoir recours à la collaboration des fournisseurs, on observe tout de même des **possibilités pour les autorités de poursuite pénale de la présente catégorie d'accéder directement, par elles-mêmes, à des données stockées à l'étranger**.

Ainsi, en **Allemagne**, on constate une controverse doctrinale quant à l'application du droit national, permettant aux autorités allemandes d'accéder à des données stockées en Allemagne, **aux cas où il n'est pas possible de savoir si elles sont stockées sur le territoire national ou bien à l'étranger**. Le pouvoir exécutif a indiqué qu'il revenait au pouvoir judiciaire de trancher cette question, ce que ce dernier n'a pas encore eu l'occasion de faire. En **France**, s'**il n'est pas avéré que des données sont stockées en dehors du territoire national** (préalablement à l'accès au contenu), les autorités de poursuite pénale peuvent, dans le cadre d'enquêtes portant sur des crimes et délits flagrants, directement accéder au contenu, en vertu du droit positif national interprété *a contrario*.

On observe par ailleurs une tendance générale au **piratage informatique**. En Italie par exemple, les autorités recourent à l'installation de virus permettant d'infecter n'importe quel ordinateur, tablette ou téléphone pour avoir accès à l'ensemble de son contenu et à toutes les informations relatives à l'usage qui en est fait ainsi qu'au son et image qui l'entourent, via le microphone et la caméra de l'appareil. Malgré le caractère répandu de cette pratique dans les juridictions étudiées, l'utilisation de cette technique pour accéder à des données stockées à l'étranger n'a pas encore fait l'objet de norme, de jurisprudence ou même, à notre connaissance, de statistiques publiques.

1.1.3. Réformes prévues

Des réformes sont envisagées au niveau européen uniquement[244]. En particulier, les institutions de l'Union européenne poursuivent leurs efforts d'amélioration de la procédure d'entraide judiciaire ; elles envisagent l'adoption d'une directive visant à améliorer l'accès transfrontière aux preuves électroniques en matière pénale ; enfin, elles évaluent la pertinence de l'intervention de l'UE pour l'encadrement du piratage informatique à des fins d'application de la loi.

1.2. Obligation de collaboration des fournisseurs

En revanche, **en Belgique**, contrairement aux Etats susmentionnés, le droit national prévoit la possibilité pour les autorités de poursuite pénale belges d'**exiger des fournisseurs de services qu'ils leur délivrent le contenu de communications électroniques**.

La jurisprudence et le droit positif national prévoit expressément que les autorités nationales belges peuvent exiger des **fournisseurs de service de communications électroniques qui mettent à disposition leurs services ou les offrent sur le territoire belge** qu'ils leur donnent accès aux communications électroniques privées. La localisation de ces entreprises ou celle du lieu de stockage des données n'entrent pas en ligne de compte. Le critère déterminant est celui du lieu où le service est offert.

Aucune réforme à venir concernant l'accès des autorités de poursuite pénale belges à des données à l'étranger contenues dans des messageries électroniques et des réseaux sociaux n'a été identifiée.

---

244 Si une réforme est prévue concernant l'accès aux données en Irlande, aucune réforme concernant l'accès à des données à l'étranger n'a été identifiée ni en Irlande, ni dans l'un des autres pays de cette catégorie.

1.3. Position indéterminée des Etats-Unis

Aux Etats-Unis, **deux courants jurisprudentiels s'opposent** à l'heure actuelle.

La Cour suprême se prononcera prochainement sur la validité d'un **courant jurisprudentiel contesté selon lequel la question qui se pose n'est pas celle de la localisation géographique du stockage des données à l'intérieur ou à l'extérieur des frontières nationales, mais de la compétence personnelle d'une instance judiciaire américaine sur une personne ayant le contrôle de ces données**. A l'heure actuelle, certaines décisions judiciaires ont établi que, lorsque la personne à même de fournir des informations n'entre pas dans cette compétence personnelle, le juge américain peut imposer à une autre personne ayant la possession, la garde ou le contrôle de ces informations, et qui elle serait soumise à sa compétence, de lui fournir ces informations, par le biais de la personne extérieure à sa compétence. La notion de contrôle sur les informations est largement interprétée dans la jurisprudence : y sont inclus le droit de, l'autorité pour et la capacité pratique d'obtenir la documentation demandée. Des instances américaines ont ainsi déjà ordonné la production d'informations en la possession d'entités étrangères, lorsqu'elles disposaient d'une compétence personnelle sur une autre entité liée ; par exemple, il a été décidé que la divulgation d'informations électroniques aux Etats-Unis extraites d'ordinateurs à l'étranger était permise en droit national américain.

Cette jurisprudence est critiquée par d'autres juges estimant qu'il s'agit d'une **application extraterritoriale inadmissible du droit américain**. Comme indiqué, la Cour suprême devrait trancher définitivement cette question dans les prochains mois, à l'occasion d'une affaire concernant l'entreprise Microsoft.

Par ailleurs, les Etats-Unis **envisagent deux modifications de leur législation**. Tout d'abord, une proposition de loi sur les données transfrontalières envisage que, après conclusion d'accords avec des Etats disposant de lois à même de garantir une protection matérielle et procédurale des droits fondamentaux, ces Etats aient le droit de requérir des données électroniques directement auprès d'entreprises américaines, sans passer par l'entraide judicaire. Réciproquement, les autorités américaines pourraient solliciter directement les entreprises établies dans l'Etat étranger partenaire. La proposition de loi encadre les cas dans lesquelles cet accès direct pourrait avoir lieu, notamment en le limitant à la prévention, la détection, l'enquête ou la poursuite de crimes graves, dont le terrorisme. Ensuite, un projet intitulé *International Communications Privacy Act* propose de permettre à une autorité étatique de demander à des fournisseurs de services en communication électronique ou de services informatiques à distance de transmettre des données relatives à des communications, même lorsque ces communications sont stockées en dehors des Etats-Unis. Pour ce faire, l'autorité étatique devrait avoir pris toutes les mesures nécessaires afin d'établir la nationalité et la localisation de l'abonné ou du consommateur dont le contenu des communications sont recherchées et qu'il y ait des raisons raisonnables de penser qu'il est américain ou physiquement présent aux Etats-Unis ou encore qu'il est ressortissant d'un Etat étranger avec lequel les Etats-Unis auraient un accord de coopération en ce sens.

2. Incrimination de l'accès direct par des autorités étrangères

Dans **l'ensemble des pays sélectionnés, aucune infraction spécifique à l'accès direct par des autorités de poursuite pénale étrangères à des données contenues dans des messageries électroniques ou des réseaux sociaux et stockées sur le territoire national concerné** n'a été identifiée.

Néanmoins, les droits pénaux nationaux **interdisent de manière générale l'accès non autorisé à ces données, en particulier en vertu de la protection de la vie privée**. La question de l'applicabilité de ces interdictions à des autorités étrangères reste sans réponse ; en l'absence d'identification de cas

concernant des autorités de poursuite pénale étrangères, les implications du **principe de souveraineté des Etats sur leur propre territoire**, défini antérieurement au développement d'Internet, sont incertaines dans la mesure où l'accès direct à des preuves électroniques ne nécessite pas le franchissement des frontières. A noter que l'**Autriche** prévoit cependant une disposition punissant pénalement l'accès à des données depuis l'étranger ; mais cette interdiction ne s'inscrit que dans le champ d'application matériel restreint du **secret des affaires et commercial**.

En revanche, on observe dans **la pratique des demandes d'accès direct auprès des fournisseurs**. En **Irlande**, le droit régissant la protection des données permet aux fournisseurs de délivrer des données lorsqu'elles sont requises pour prévenir, détecter ou enquêter sur des infractions ou appréhender ou poursuivre leurs auteurs. Des entreprises comme Facebook ou Microsoft interprètent cette exception prévue par le droit irlandais de la protection des données comme les autorisant, sur une base volontaire, à délivrer des données de connexion ; elles exigent au contraire **l'exequatur par les autorités irlandaises pour la transmission de données comportant du contenu** (tel que des messages ou des photos), faute de quoi l'autorité étrangère verra sa demande rejetée par l'entreprise. La **Belgique** prévoit expressément la possibilité pour une autorité étrangère (ayant conclu un accord en ce sens avec la Belgique et sous condition de validation rétroactive par les autorités belges notamment) de prendre connaissance de communications électroniques privées lorsque cette autorité étrangère mène une enquête pénale visant **une personne qui se trouve sur le territoire belge**.

V. TABLEAU COMPARATIF DES RAPPORTS NATIONAUX

	Entraide judiciaire	**Accès direct aux contenus par les autorités prévu dans la loi (hors possibilités prévues par la Convention du Conseil de l'Europe sur la cybercriminalité)**	**Accès direct via les fournisseurs : possibilité de les contraindre (hors possibilités prévues par la Convention du Conseil de l'Europe sur la cybercriminalité)**	**Réformes prévues (hors droits européens)**	**Incrimination générale / Protection de la vie privée**	**Incrimination spécifique des autorités de poursuite pénale étrangères**
Allemagne	Oui	Seule possibilité (controversée) : lorsqu'il n'est pas possible de savoir si les données sont stockées sur le territoire national ou à l'étranger	Non	Non	Oui	Non
Autriche	Oui	Non	Non	Non	Oui	Non
Belgique	Oui	Inconnu	Oui, pour certaines infractions, les autorités belges peuvent exiger des fournisseurs qui mettent à disposition leurs services ou les offrent sur le territoire belge qu'ils donnent accès aux communications électroniques privées (la localisation de ces entreprises ou celle du lieu de stockage des données n'entrent pas en ligne de compte).	Non	Oui	Non
Etats-Unis	Oui	Non	Oui (pas encore définitivement tranché),	1/ Proposition de loi sur les données	Oui	Non

			lorsque la personne ayant le contrôle des données entre dans le champ de compétence personnelle d'une instance judiciaire américaine, ou bien lorsqu'une autre personne ayant le contrôle (sens large : droit, autorité, capacité pratique) des données et se trouvant sous sa juridiction est en mesure de fournir ces données par le biais d'une personne extérieure à sa compétence.	transfrontières : conclusion d'accords avec des Etats octroyant un droit réciproque de requérir des données électroniques directement auprès des entreprises établies dans l'autre Etat (limitation aux crimes graves). 2/*International Communications Privacy Act* : une autorité étatique pourrait demander à des fournisseurs de services en communication électronique ou de services informatiques à distance de transmettre des données relatives à des communications, même stockées à l'étranger (limitation aux Américains, personnes physiquement présentes aux USA ou ressortissants d'Etats étrangers parties à un		

				accord de coopération spécifique).		
France	Oui	Seule possibilité : lorsque, préalablement à l'accès au contenu, il n'est pas avéré que les données sont stockées à l'étranger (limitation aux crimes et délits flagrants).	Non	Non	Oui	Non
Irlande	Oui	Non	Non	Non	Oui	Non
Italie	Oui	Non	Non	Non	Oui	Non

INSTITUT SUISSE DE DROIT COMPARÉ

Dr. Lukas Heckendorn Urscheler
Vice-directeur

Cheffe de projet	Carole Viennet *Conseillère juridique, ordres juridiques francophones*
Union européenne et Conseil de l'Europe	Anne-Carine Pierrat *Stagiaire* Carole Viennet *Conseillère juridique, ordres juridiques francophones*
Allemagne	Isabelle Blatter *Stagiaire* Dr. Johanna Fournier, LLM *Conseillère juridique, ordres juridiques germanophones*
Autriche	Dr. Johanna Fournier, LLM *Conseillère juridique, ordres juridiques germanophones*
Belgique	Sylvain Tscheulin *Stagiaire* Carole Viennet *Conseillère juridique, ordres juridiques francophones*
Etats-Unis	Karen Topaz Druckman, LLM *Conseillère juridique, droit des Etats-Unis*
France	Anne-Carine Pierrat *Stagiaire* Carole Viennet *Conseillère juridique, ordres juridiques francophones*
Irlande	John Curran, LLM *Conseiller juridique, Common Law*
Italie	Dr. Ilaria Pretelli *Conseillère juridique, droit italien*