Version provisoire, 3 mai 2016
Strasbourg, France

T-CY (2016)2
Provisoire

Comité de la Convention cybercriminalité (T-CY)

Accès de la justice pénale aux données stockées dans le Cloud :

la coopération avec des fournisseurs de services "étrangers"

Document de synthèse

préparé par le Groupe sur les preuves dans le Cloud

www.coe.int/TCY

Table des matières

Personne à contacter
Alexander Seger
Secrétaire exécutif du Comité de la Convention cybercriminalité (T-CY) Tél : +33-3-9021-4506
Direction Générale des Droits de l'homme et de l'État de droit Fax : +33-3-9021-5650
Conseil de l'Europe, Strasbourg, France Email : alexander.seger@coe.int

1 But de ce rapport

Le Comité de la Convention cybercriminalité (T-CY), lors de sa 12ème plénière (2-3 décembre 2014), a créé un groupe de travail pour examiner les moyens d'accès de la justice pénale aux preuves dans le Cloud, y compris au moyen de l'entraide judiciaire (« Groupe sur les preuves dans le Cloud »)[1]. Le Groupe sur les preuves dans le Cloud a été chargé de soumettre avant décembre 2016 un rapport au T-CY présentant des options et des recommandations pour la poursuite de l'action en ce domaine.

En 2015, le Groupe sur les preuves dans le Cloud du T-CY, suite à un document de travail présentant succinctement les défis qui se posent en matière d'accès de la justice pénale aux données stockées dans le Cloud (publié en mai 2015 et discuté lors de la Conférence Octopus en juin 2015), a tenu une audition pour les fournisseurs de services le 30 novembre 2015 qui a porté sur la coopération directe des autorités de justice pénale avec les prestataires de services basés dans des juridictions étrangères.

Il est fréquent qu'une autorité de poursuite ou de police (« service répressif ») d'une Partie à la Convention de Budapest requière d'un fournisseur de services d'une autre juridiction des données en relation avec une enquête pénale particulière. Le plus souvent, il s'agit d'obtenir des informations sur un abonné de fournisseurs de services multinationaux dont le siège se trouve aux États-Unis (« fournisseurs de services basés aux États-Unis »). Certains de ces prestataires de services ont des filiales en Europe ou ailleurs.

Les rapports de transparence publiés par les fournisseurs de services basés aux États-Unis indiquent qu'ils répondent de manière positive à environ 60% de ces demandes « de façon volontaire ».

L'article 18 de la Convention de Budapest couvre l'« injonction de produire » et l'article 18.1.b traite spécifiquement de la production d'informations relatives aux abonnés par un fournisseur de services « offrant des prestations sur le territoire de la Partie » :

> Article 18 - Injonction de produire
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
>
> a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et
>
> b à un fournisseur de services offrant des prestations sur le territoire de la Partie de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Le Rapport explicatif (paragraphe 171) de la Convention de Budapest indique que l'article 18 vise aussi à couvrir les situations de coopération volontaire :

> 171. Une « injonction de produire » constitue une mesure souple que les services répressifs peuvent mettre en œuvre dans bien des situations, en particulier dans les cas où il n'est pas nécessaire de recourir à une mesure plus contraignante ou plus onéreuse. L'instauration d'un tel mécanisme procédural sera aussi utile pour les tiers gardiens des données qui, tels les fournisseurs d'accès Internet, sont souvent disposés à collaborer avec les services répressifs sur une base volontaire en leur fournissant les données sous leur contrôle, mais préfèrent disposer

[1] Document T-CY(2014)16, Accès transfrontalier aux données et compétence : options concernant l'action future du T-CY (rapport du Groupe ad hoc sur l'accès transfrontalier aux données, adopté par la 12e Plénière du T-CY, décembre 2014).

d'une base juridique appropriée pour apporter cette aide, les déchargeant de toute responsabilité contractuelle ou autre.

Le présent document de synthèse vise à fournir un aperçu[2] des politiques et des pratiques de certains grands fournisseurs de services basés aux États-Unis en matière de divulgation « volontaire » d'informations aux services répressifs de juridictions étrangères[3] et à faciliter ainsi la discussion sur les options futures concernant l'accès de la justice pénale aux preuves électroniques dans le Cloud.

2 La coopération directe avec des fournisseurs étrangers

2.1 Fréquence des demandes directes adressées à des fournisseurs de services basés aux États-Unis par des Parties à la Convention de Budapest

Depuis plusieurs années, de nombreux fournisseurs de services dont le siège se trouve aux États-Unis ont commencé à publier des « rapports de transparence » sur les demandes de données reçues de gouvernements aux fins de la lutte contre la criminalité. La divulgation volontaire de « fichiers d'abonnés » – et des contenus de leurs communications dans les cas d'urgence – est possible aux termes du droit des États-Unis et, spécifiquement, de la loi sur les communications électroniques (*Electronic Communications Privacy Act*)[4].

Les chiffres de 2014 concernant six de ces fournisseurs de services (Apple, Facebook, Google, Microsoft, Twitter et Yahoo) montrent que 45 des 48 Parties à la Convention de Budapest[5] ont envoyé des demandes d'information à un ou plusieurs d'entre eux. Les Parties à la Convention (États-Unis inclus) ont envoyé en tout environ 190 000 demandes. Les Parties à la Convention autres que les États-Unis ont envoyé environ 109 000 demandes à ces six fournisseurs de services basés aux États-Unis et, dans au moins 65 000 cas (60% des demandes), ont reçu au moins certaines des données demandées. Les données provisoires pour 2015 présentent un tableau analogue.

Dans presque tous les cas, les données demandées et divulguées étaient des informations sur un usager ou un compte, c'est-à-dire principalement des informations relatives à des abonnés. Des contenus ont rarement été demandés ou divulgués.

Ces chiffres ne couvrent pas encore les demandes directes de suppression de contenus ou d'informations sur des appareils[6] ou les demandes envoyées directement à de nombreux autres fournisseurs de services.

[2] N.B. : les politiques et les pratiques des fournisseurs de services ont fréquemment changé, y compris pendant la préparation du présent rapport.
[3] La question du champ d'application de l'article 18 sera abordée plus en détail dans un rapport distinct.
[4] 18 U.S. Code § 2702, https://www.law.cornell.edu/uscode/text/18/2702
[5] Les exceptions sont l'Azerbaïdjan, Maurice et « l'ex-République yougoslave de Macédoine ». Les données provisoires pour 2015 indiquent que l'Azerbaïdjan et « l'ex-République yougoslave de Macédoine » ont aussi envoyé des demandes pendant cette année.
[6] En 2014, par exemple, les Parties à la Convention autres que les États-Unis ont envoyé à Apple près de 27 000 demandes portant sur plusieurs centaines de milliers d'appareils.

	Demandes de données envoyées à Apple, Facebook, Google, Microsoft, Twitter et Yahoo en 2014[7]		
Parties à la Convention	**Nombre de demandes reçues**	**Nombre de divulgations**	**%**
Albanie	24	7	29%
Arménie	11	2	18%
Australie	6 438	4 236	66%
Autriche	246	73	30%
Azerbaïdjan	-	-	
Belgique	1 804	1 316	73%
Bosnie-Herzégovine	13	8	62%
Bulgarie	5	3	60%
Canada	850	477	56%
Croatie	45	34	76%
Chypre	38	21	55%
République tchèque	333	204	61%
Danemark	362	225	62%
République dominicaine	54	30	56%
Estonie	35	19	54%
Finlande	144	102	71%
France	21 772	12 863	59%
Géorgie	1	0	0%
Allemagne	25 519	13 801	54%
Hongrie	345	159	46%
Islande	3	2	67%
Italie	9 365	4 620	49%
Japon	1 617	1 010	62%
Lettonie	2	2	100%
Lichtenstein	5	1	20%
Lituanie	49	28	57%
Luxembourg	153	117	76%
Malte	377	197	52%
Maurice	-	-	
Moldova	13	7	54%
Monténégro	7	1	14%
Pays-Bas	1 099	856	78%
Norvège	363	238	65%
Panama	88	68	77%

[7] Source : Rapports de transparence :
Apple : http://www.apple.com/privacy/transparency-reports/
Facebook : https://govtrequests.facebook.com/about/#
Google : https://www.google.com/transparencyreport/
Microsoft : https://www.microsoft.com/about/csr/transparencyhub/
Twitter : https://transparency.twitter.com/
Yahoo : https://transparency.yahoo.com/government-data-requests

	Demandes de données envoyées à Apple, Facebook, Google, Microsoft, Twitter et Yahoo en 2014[7]		
Parties à la Convention	**Nombre de demandes reçues**	**Nombre de divulgations**	**%**
Pologne	1 747	550	31%
Portugal	2 223	1 356	61%
Roumanie	80	40	50%
Serbie	16	9	56%
Slovaquie	107	36	34%
Slovénie	11	6	55%
Espagne	4 462	2 391	54%
Sri Lanka	1	-	0%
Suisse	462	266	58%
« L'ex-Rép. yougoslave de Macédoine »	-	-	
Turquie	8 405	5 625	67%
Ukraine	8	2	25%
Royaume-Uni	20 127	13 894	69%
États-Unis	80 703	63 147	78%
Total, États-Unis non inclus	**108 829**	**64 901**	**60%**
Total, États-Unis inclus	**189 532**	**128 048**	**68%**

Ces chiffres montrent que les demandes de données sont très inégales selon les pays :

- La France, l'Allemagne et le Royaume-Uni ont envoyé chacun directement plus de 20 000 demandes aux six fournisseurs de services, alors que la Bulgarie, l'Islande, la Lettonie, le Lichtenstein, la Géorgie, le Monténégro, le Sri Lanka et l'Ukraine en ont envoyé moins de 10 et l'Azerbaïdjan, Maurice et « l'ex-République yougoslave de Macédoine » aucune en 2014. Les données provisoires pour 2015 indiquent que l'Azerbaïdjan et « l'ex-République yougoslave de Macédoine » ont aussi envoyé des demandes pendant cette année.

- Le nombre de divulgations partielles ou complètes de données varie entre les six fournisseurs de services : Microsoft est le fournisseur qui donne le plus fréquemment suite aux demandes d'informations (dans 78% des cas pour les Parties à la Convention autres que les États-Unis), suivi par Google (54%), Facebook (48%) et Apple (38%) ; Yahoo (34%) et Twitter (21%) sont les fournisseurs qui répondent le moins souvent de manière positive aux demandes. Yahoo rejette la plupart des demandes d'informations en invoquant d'autres motifs que la non-disponibilité des données[8].

[8] « Yahoo pouvait être en possession de données correspondant à la demande d'un gouvernement mais ces données n'ont pas été produites en raison d'un défaut ou d'une insuffisance de la demande (par ex. l'organe gouvernemental concerné cherchait à obtenir des informations échappant à sa compétence juridictionnelle ou bien la demande portait uniquement sur des données qui ne pouvaient être obtenues légalement au moyen de la procédure légale utilisée). Cette catégorie inclut aussi les demandes de données émanant d'un gouvernement qui ont été retirées après leur réception par Yahoo. Nous vérifions soigneusement la validité juridique des demandes de données que nous recevons de gouvernements et nous les interprétons de manière restrictive en vue de produire la quantité minimale de données requise pour satisfaire à ces demandes. »
https://transparency.yahoo.com/faq/index.htm#list_item_4

- Les six fournisseurs coopèrent de façon très inégale avec les différentes Parties à la Convention. Du point de vue des taux de divulgation, par exemple :

  - Google coopère à un degré supérieur à la moyenne avec la Finlande (83%), les Pays-Bas (81%) et le Japon (79%) et à un degré inférieur à la moyenne avec la Pologne (29%) et la Slovaquie (8%), mais pas du tout avec la Hongrie (0%) et la Turquie (0%) ;
  - Microsoft, par contre, coopère assez bien avec la Hongrie (83%) et la Turquie (76%) ;
  - Facebook répond aussi assez bien aux demandes de la Hongrie (83%) et de la Turquie (66%), mais moins à celles de la Pologne (29%), du Portugal (38%) et de l'Espagne (37%) ;
  - Yahoo coopère avec l'Australie (51%) mais ne répond pas du tout aux demandes des Pays-Bas, de la Norvège, du Portugal et de la Suisse ;
  - Microsoft, en revanche, coopère assez bien avec les Pays-Bas (83%), la Norvège (82%), le Portugal (85%) et la Suisse (74%) ;
  - Twitter coopère à un degré supérieur à la moyenne avec l'Australie (58%), le Japon (36%) et la Norvège (50%), mais pas du tout avec la Turquie (0%) et à un degré inférieur à la moyenne avec la France (11%), l'Allemagne (16%) et l'Espagne (12%).

- Les écarts en matière de réponse aux demandes des Parties à la Convention apparaissent aussi clairement dans les données publiées par Google sur les suppressions de contenus : en 2014, Google/You Tube ont supprimé des contenus suite à 49% des plus de 14 000 demandes reçues de Parties autres que les États-Unis. Le taux de réponse aux demandes reçues de la France (76%) ou de l'Italie (73%) contraste fortement avec celui concernant les demandes reçues de la Turquie (35%) ou de l'Australie (33%).

- Une remarque importante s'impose au sujet des demandes de suppression de contenus par Google/You Tube : le fait qu'une demande se fonde ou non sur une décision de justice semble assez peu pertinent. Les demandes reposant sur une décision de justice aboutissent à une suppression de contenus dans 53% des cas, alors que la moyenne générale est de 49%.

- Les six fournisseurs de services pris en compte dans le présent rapport ne permettent pas d'établir un tableau complet de la situation. Des demandes sont aussi envoyées à de nombreux autres fournisseurs. Par exemple, Snapchat[9] – pendant la période de janvier à juin 2015 – a reçu 82 demandes de Parties à la Convention autres que les États-Unis (Australie, Canada, Danemark, Espagne, France, Norvège, République tchèque et Royaume-Uni) mais n'a répondu qu'aux requêtes urgentes (en produisant des données dans 73% des requêtes urgentes).

[9] https://www.snapchat.com/transparency/

2.2 Politiques et procédures des fournisseurs de services

2.2.1 Directives à l'intention des services répressifs

2.2.1.1 Apple

Apple publie et met à jour des directives sur les requêtes des services répressifs des États-Unis, de l'Europe/Moyen-Orient/Inde/Afrique et du Japon/Asie-Pacifique[10]. D'après ces directives, « aucune divulgation ne peut avoir lieu sans une procédure légale régulière … ».

Aux États-Unis :

> Apple accepte la notification par courrier électronique des injonctions, mandats de perquisition et requêtes judiciaires d'information, à condition qu'ils soient transmis depuis l'adresse électronique officielle du service de lutte contre la criminalité concerné[11].

Dans la région Europe/Moyen-Orient/Inde/Afrique :

> Apple considère qu'une demande d'information d'un service de lutte contre la criminalité est légalement valide si elle est effectuée dans un contexte lié à la prévention de bonne foi, à la détection ou à l'investigation des infractions et répondra de manière appropriée aux demandes qu'il juge remplir ces conditions[12].

Dans la région Japon/Asie-Pacifique :

> Apple considère qu'un document judiciaire est valide s'il s'agit d'une lettre de coopération, d'une notification aux fins de l'obtention d'éléments de preuve, d'une injonction, d'une décision judiciaire, d'un mandat de perquisition et de saisie, d'une lettre d'autorisation au titre de la loi australienne sur les télécommunications de 1979 ou de l'équivalent local, légalement valide, de tels documents. Le type de document exigé par Apple peut varier d'un pays à l'autre et dépend de l'information recherchée[13].

Apple Ireland est responsable de l'Union européenne et de la Suisse. Apple considère que le droit irlandais s'applique aux métadonnées et le droit des États-Unis aux données de contenu, car ces dernières sont stockées aux États-Unis.

Selon l'Engagement de confidentialité d'Apple[14] :

> Utilisateurs internationaux
> Toutes les informations que vous divulguez pourront être transférées ou seront accessibles par des sociétés à travers le monde, comme décrit dans le présent Engagement de confidentialité. Apple se conforme aux principes « Safe Harbor » définis par le ministère américain du commerce en matière de collecte, d'utilisation et de conservation des informations personnelles collectées par des sociétés de l'Espace économique européen et de Suisse. Vous trouverez ici de plus amples informations sur le programme « Safe Harbor » du ministère américain du commerce.

[10] http://www.apple.com/privacy/government-information-requests/
[11] http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf
[12] http://images.apple.com/privacy/docs/legal-process-guidelines-emeia.pdf
[13] http://images.apple.com/privacy/docs/legal-process-guidelines-apac.pdf
[14] http://www.apple.com/legal/privacy/en-ww/. Ce site – consulté le 3 mars 2016 – mentionne toujours le programme « Safe Harbor » qui, à cette date, était déjà interrompu. Il porte la mention « Dernière mise à jour : 17 septembre 2014 ».

> Veuillez noter que les informations personnelles, y compris les informations fournies lors de l'utilisation d'iCloud, concernant les individus résidant dans un État membre de l'Espace économique européen (EEE) et en Suisse sont contrôlées par Apple Distribution International, à Cork (Irlande), et traitées pour son compte par Apple Inc. Les informations personnelles recueillies au sein de l'EEE et de la Suisse lors de l'utilisation d'iTunes sont contrôlées par iTunes SARL, au Luxembourg, et traitées pour son compte par Apple Inc.

2.2.1.2 Facebook

Facebook publie des directives opérationnelles à l'intention des services répressifs[15].

En ce qui concerne les demandes émanant des autorités des États-Unis :

- Facebook « divulgue les fichiers de compte exclusivement en conformité avec nos conditions d'utilisation et la législation applicable, y compris la loi fédérale SCA (*Stored Communications Act*, 18 U.S.C. §§ 2701-2712) ».

En ce qui concerne les demandes internationales :

- Facebook « divulgue les fichiers de compte exclusivement en conformité avec nos conditions d'utilisation et la législation applicable. Un traité d'entraide judiciaire ou une lettre rogatoire peut être requise pour exiger la divulgation des contenus d'un compte ».

Facebook Ireland Limited est une filiale de Facebook Inc. Tous les utilisateurs de Facebook en dehors des États-Unis et du Canada ont apparemment un contrat avec Facebook Ireland Limited[16].

Facebook[17] indique dans sa Politique d'utilisation des données :

> Nous pourrons accéder à vos données personnelles, les conserver et les partager en réponse à une demande légale (mandat de perquisition, ordonnance d'un tribunal ou autre) si nous pensons en toute bonne foi que la loi nous y oblige. Cela peut inclure la réponse à des demandes légales provenant de juridictions extérieures aux États-Unis, lorsque nous avons toutes les raisons de penser que cette réponse est requise par la législation de la juridiction concernée, qu'elle s'applique aux utilisateurs dépendant de cette juridiction et qu'elle est conforme aux normes internationalement reconnues.

Facebook peut donc répondre à une demande internationale émise au titre des normes du droit interne de l'État requérant.

Facebook maintient un portail spécifique pour les demandes des services répressifs et publie des rapports de transparence sur les demandes des gouvernements[18].

2.2.1.3 Google

Google publie des directives à l'intention des services répressifs. Ces directives fournissent aussi des indications aux utilisateurs de Google sur la manière dont les autorités de justice pénale peuvent obtenir accès à leurs données[19].

[15] https://www.facebook.com/safety/groups/law/guidelines/
[16] https://en.wikipedia.org/wiki/Facebook
[17] https://govtrequests.facebook.com/
[18] https://www.facebook.com/about/privacy/other
[19] https://www.google.com/transparencyreport/userdatarequests/legalprocess/

Google peut fournir les données des utilisateurs de comptes Gmail, YouTube, Google Voice et Blogger.

Google déclare qu'il répond aux demandes de données d'un utilisateur si la demande est conforme aux normes légales et à la politique de Google, c'est-à-dire si elle est effectuée par écrit, signée par un représentant autorisé de l'organe demandeur et émise au titre d'un texte de loi pertinent.

Pour les demandes de divulgation des données d'un utilisateur reçues des autorités des États-Unis, Google exige une injonction, une décision judiciaire ou un mandat de perquisition, selon le type de données demandées.

Dans le cas des demandes émanant d'un autre pays, Google peut divulguer des données si la demande s'inscrit dans une procédure d'entraide judiciaire. Cependant, Google indique[20] :

> Nous pouvons fournir volontairement des données concernant un utilisateur en réponse à une procédure légale valide émanant d'un organe gouvernemental d'un pays autre que les États-Unis si la demande est conforme aux normes internationales, à la législation des États-Unis, à la politique de Google et au droit de l'État demandeur.

2.2.1.4 Microsoft

Microsoft publie deux fois par an un rapport sur les demandes de données d'utilisateurs émanant de services répressifs[21].

Microsoft déclare que toute demande des données relatives à un client de Microsoft émanant d'un gouvernement doit être effectuée conformément à la procédure légale applicable, c'est-à-dire qu'elle doit s'appuyer sur une ordonnance judiciaire ou un mandat de perquisition pour les données de contenu, ou sur une injonction de produire les informations relatives à un abonné ou d'autres métadonnées, et que la demande doit viser un compte spécifique.

Lorsqu'elle reçoit une demande de données, l'équipe de conformité de Microsoft examine la demande, contrôle sa validité et la rejette si elle la juge non valide.

Microsoft peut rejeter ou contester une demande de données pour plusieurs raisons, parmi lesquelles :

- la demande excède les pouvoirs de l'organe requérant ;
- l'information demandée échappe à la compétence du gouvernement ou de l'organe requérant ;
- la demande n'est pas signée ou autorisée ;
- la demande est de portée trop étendue.

2.2.1.5 Twitter

Twitter publie des directives à l'intention des services répressifs[22]. Ces directives fournissent des indications sur les données de compte disponibles, la rétention des données, les demandes de conservation de données, les demandes d'information sur les comptes Twitter, les demandes d'urgence et l'entraide judiciaire.

[20] https://www.google.com/transparencyreport/userdatarequests/legalprocess/
[21] https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/
[22] https://support.twitter.com/articles/41949#

Twitter peut aussi fournir des données sur les comptes d'utilisateurs des services Periscope[23] et Vine[24]. Les services répressifs doivent adresser leurs demandes d'informations relatives à des comptes d'utilisateurs à Twitter Inc. (San Francisco, Californie) ou à Twitter International Company à Dublin (Irlande). Twitter répond aux demandes légales valides émises conformément à la législation applicable.

Les informations à caractère non public concernant des utilisateurs de Twitter ne peuvent être divulguées à un service de lutte contre la criminalité qu'en réponse à une procédure légale adéquate telle qu'une injonction, une ordonnance judiciaire ou une autre mesure légale valide – ou en réponse à une demande d'urgence valide.

2.2.1.6 Yahoo

Yahoo publie des rapports de transparence biannuels sur les demandes de données émanant de gouvernements[25], ainsi que des « principes mondiaux sur la voie à suivre pour répondre aux demandes de gouvernements » (*Yahoo Global Principles for Responding to Government Requests*)[26].

Yahoo a publié des directives à l'intention des services répressifs[27], qui exigent le respect des normes de la loi ECPA (*Electronic Communications Privacy Act*, 18 U.S.C. §§ 2501 et suiv. et 18 U.S.C. § 2703) s'appliquant à la divulgation de l'information essentielle relative aux abonnés, des contenus et d'autres fichiers clients.

En outre, Yahoo exige que :

- le compte d'utilisateur visé par la demande soit spécifiquement identifié dans la procédure légale au moyen de l'identifiant de l'utilisateur, de l'adresse électronique, d'un pseudonyme ou d'un autre identifiant adéquat ;
- toutes les demandes soient soumises par écrit, sauf si la législation applicable autorise explicitement les demandes orales ;
- toutes les demandes soient adressées sur papier à en-tête officiel et accompagnées d'informations suffisantes pour permettre de vérifier qu'elles émanent d'une personne ou d'un organe autorisé à effectuer une telle demande.

2.2.2 Types de données disponibles et procédures et conditions de divulgation

2.2.2.1 Apple

Dans le cas d'une demande des États-Unis, Apple peut fournir les informations suivantes sur la base d'un ordre/injonction de produire :

[23] https://www.periscope.tv/
[24] https://vine.co/
[25] https://transparency.yahoo.com/
[26] https://transparency.yahoo.com/principles
[27] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm. Ce site n'était plus accessible à la fin mars 2016. Le lien qui suit permet d'accéder au « guide de conformité de Yahoo pour les organes répressifs » (*Yahoo! Compliance Guide For Law Enforcement*) :
http://r.search.yahoo.com/_ylt=AwrBTzwtAflWGCYA5vpXNyoA;_ylu=X3oDMTEydTYzYW4wBGNvbG8DYmYxBHBvcwMyBHZ0aWQDQTAxOTZfMQRzZWMDc3I-/RV=2/RE=1459188141/RO=10/RU=https%3a%2f%2fwww.eff.org%2ffiles%2ffilenode%2fsocial_network%2fyahoo_sn_leg-doj.pdf/RK=0/RS=6PiFEwB8arANWnhrQwZeY5adxk8-

- données de base (nom, adresse physique, adresse électronique et numéro de téléphone) d'un abonné à un compte iCloud[28] et journaux de connexion conservés jusqu'à 30 jours,
- données essentielles ou informations client (nom, adresse physique, adresse électronique et numéro de téléphone) liées à l'enregistrement d'un appareil Apple,
- fichiers services d'un client en relation avec les appareils ou les services utilisés par un client,
- renseignements sur un abonné iTunes et journaux de connexion avec les adresses IP,
- renseignements sur un abonné (y compris le numéro de carte de paiement) en relation avec les transactions effectuées dans les magasins de détail Apple ou les achats en ligne,
- journaux de connexion iPhone,
- adresses MAC (*Media Access Control*) des appareils,
- adresses IP et autres identifiants pour l'activation d'appareils iOS ;

sur la base d'une ordonnance d'un tribunal au titre de la loi 18 U.S.C. § 2703(d) ou d'une ordonnance judiciaire répondant à une norme similaire :

- données de trafic iTunes (registres des transactions telles qu'achats ou téléchargements),
- données de trafic liées à un compte de courrier électronique (journaux de messagerie ou *mail logs*), y compris les connexions entrantes et sortantes et l'adresse électronique des destinataires,
- journaux des communications d'appel FaceTime ;

sur la base d'un mandat de perquisition émis après établissement d'une cause probable :

- contenus spécifiques iTunes achetés ou téléchargés,
- courriers électroniques ou autres contenus iCloud tels que photos, documents, calendriers, paramètres d'appareils, iMessage, SMS, messagerie vocale, etc. Les contenus iCloud sont chiffrés à l'emplacement du serveur et « Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis »,
- extraction de données d'appareils iOS à accès contrôlé par mot de passe (seulement en dessous de l'iOS 8.0). Cette extraction peut être effectuée au siège d'Apple en Californie. Les appareils doivent y être apportés ou envoyés.

Les directives pour la région Europe/Moyen-Orient/Inde/Afrique indiquent que les informations suivantes peuvent être fournies :

- renseignements sur un abonné d'iCloud, y compris les journaux de connexion qui sont conservés 30 jours et peuvent être communiqués en réponse à une « demande légalement valide » ;
- les journaux de messagerie iCloud mail qui sont conservés jusqu'à 60 jours et peuvent être communiqués en réponse à une « demande légalement valide » ;
- les courriers électroniques et d'autres contenus iCloud, qui peuvent être fournis « uniquement en réponse à un mandat de perquisition émis conformément à la procédure MLAT » ;
- des informations sur les appareils comme l'adresse MAC (*Media Access Control*) ou l'identifiant UDID (*Unique Device Identifier*), en réponse à une « demande légalement valide » ;
- les journaux d'accès (*sign-on logs*), en réponse à une « demande légalement valide ».

[28] Apple exige un identifiant Apple/compte de courrier électronique ou des renseignements sur l'abonné tels que nom et prénom, numéro de téléphone et adresse du domicile pour identifier un compte.

En ce qui concerne les procédures :

> Apple accepte les notifications par courrier électronique de demandes d'information légalement valides, à condition qu'elles soient transmises depuis l'adresse électronique officielle du service de lutte contre la criminalité concerné. Les agents de ces services dans la région Europe/Moyen-Orient/Inde/Afrique qui soumettent une demande d'information à Apple doivent utiliser un formulaire type de demande d'information (*Law Enforcement Information Request*, http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf) et l'envoyer directement depuis l'adresse électronique officielle de leur service à : law.enf.emeia@apple.com. Cette adresse électronique doit être utilisée uniquement pour la soumission de demandes légales de services répressifs et d'agents gouvernementaux.

Sauf en cas de procédure d'urgence, Apple ne divulgue des contenus que sur la base d'un mandat de perquisition émis conformément à une requête d'entraide judiciaire ou à une mesure de coopération similaire.

En ce qui concerne iTunes, les demandes de renseignements sur un abonné et les demandes de journaux de connexion IP doivent être envoyées pour validation au Procureur général du Luxembourg, qui les transmet ensuite à iTunes pour réponse.

Cependant, dans la région Japon/Asie-Pacifique :

> Lorsqu'un client ouvre un compte iTunes, les renseignements de base comme le nom, l'adresse physique, l'adresse électronique et le numéro de téléphone peuvent être fournis. En outre, des informations sur les transactions d'achat/téléchargement et connexions iTunes, les journaux de connexion de l'abonné iTunes, avec les adresses IP et d'autres informations, peuvent être obtenues sur la base d'un document émis conformément à la procédure légale adéquate par le pays demandeur[29].

2.2.2.2 Facebook

Facebook peut fournir les données suivantes en réponse aux demandes provenant des États-Unis :

sur la base d'un ordre/injonction de produire émis en relation avec une enquête spécifique :

- les renseignements de base sur l'abonné [définis dans la loi 18 U.S.C. § 2703(c)(2)], qui peuvent inclure : le nom, la durée du service, le numéro de la carte de crédit, la ou les adresses électroniques et, le cas échéant, une ou plusieurs adresses IP de connexion/déconnexion récentes ;

sur la base d'une ordonnance judiciaire :

- certains fichiers ou d'autres informations relatives au compte – à l'exclusion du contenu des communications – qui peuvent inclure, outre les renseignements de base sur l'abonné, des en-têtes de message et des adresses IP ;

[29] http://images.apple.com/privacy/docs/legal-process-guidelines-apac.pdf

sur la base d'un mandat de perquisition ou document similaire émis après établissement d'une cause probable :

- les contenus stockés relatifs à un compte, qui peuvent inclure des messages, des photos, des vidéos, des affichages muraux et des données de localisation ;

sur la base de *National Security Letters* :

- le nom et la durée du service.

Les demandes provenant de régions autres que les États-Unis/Canada doivent être envoyées à Facebook Ireland et sont traitées par le service spécialisé (*Law enforcement unit*) de Facebook Ireland. Les conditions et procédures de Facebook pour la divulgation de données à des autorités étrangères ne sont pas très détaillées.

Il semblerait que Facebook Ireland Limited puisse divulguer sur demande des informations sur les abonnés (et « certaines autres données », c'est-à-dire les données de trafic).

Facebook ne traite pas les demandes de portée étendue ou formulées en termes vagues.

> Toutes les demandes doivent décrire spécifiquement les données requises et comprendre les éléments suivants :
> - le nom de l'autorité émettrice, le numéro de badge/d'identification de l'agent responsable, une adresse électronique appartenant au domaine d'un service de lutte contre la criminalité et un numéro de téléphone à contacter directement ;
> - l'adresse électronique, le numéro d'identification de l'utilisateur (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) ou l'identifiant (http://www.facebook.com/username) du profil Facebook.

Les demandes doivent être transmises via le système de demande en ligne (*Law Enforcement Online Request System*) à : facebook.com/records.

2.2.2.3 Google

Google peut fournir les données suivantes en réponse à une demande provenant d'une autorité des États-Unis :

sur la base d'un ordre/injonction de produire :

- données d'enregistrement de l'abonné et adresses IP de connexion avec l'horodatage correspondant pour les comptes Gmail et YouTube,
- données d'enregistrement de l'abonné, adresses IP de connexion avec l'horodatage correspondant, fichiers de connexion téléphonique et données de facturation pour les comptes Google Voice,
- page d'enregistrement du blog et informations sur le propriétaire/abonné pour Blogger ;

sur la base d'une ordonnance judiciaire :

- données autres que les contenus et informations pouvant être obtenues au moyen d'une injonction pour les comptes Gmail,

- adresse IP de téléchargement de vidéo avec l'horodatage correspondant et informations pouvant être obtenues au moyen d'une injonction pour les comptes YouTube,
- numéro de transfert d'appel et informations pouvant être obtenues au moyen d'une injonction pour les comptes Google Voice,
- adresse IP et horodatage correspondant à un billet de blog spécifié, adresse IP et horodatage correspondant à un commentaire de blog spécifié et informations pouvant être obtenues au moyen d'une injonction pour les comptes Blogger ;

sur la base d'un mandat de perquisition :

- contenu de courriers électroniques et informations pouvant être obtenues au moyen d'une injonction ou d'une ordonnance judiciaire pour les comptes Google,
- copie d'une vidéo privée et informations vidéo associées, contenu de message privé pouvant être obtenus au moyen d'une injonction ou d'une ordonnance judiciaire pour les comptes YouTube,
- contenu de messages stockés, contenu de messages vocaux stockés pouvant être obtenus au moyen d'une injonction ou d'une ordonnance judiciaire pour les comptes Google Voice,
- contenu de billets et commentaires de blog privé pouvant être obtenus au moyen d'une injonction ou d'une ordonnance judiciaire pour les comptes Blogger.

Les demandes de données doivent être effectuées par écrit, signées par un représentant autorisé de l'organe demandeur et émises conformément à la législation pertinente.

Pour les demandes provenant de l'extérieur des États-Unis, Google peut fournir des données identiques à celles indiquées ci-dessus à condition que la demande passe par une procédure d'entraide judiciaire.

Cependant,

> Nous pouvons fournir volontairement des données concernant un utilisateur en réponse à une procédure légale valide émanant d'un organe gouvernemental d'un pays autre que les États-Unis si la demande est conforme aux normes internationales, à la législation des États-Unis, à la politique de Google et au droit de l'État demandeur[30].

2.2.2.4 Microsoft

Dans le cas des demandes provenant des États-Unis, Microsoft peut fournir :

- des données autres que les contenus, à savoir les renseignements de base sur l'abonné (adresse électronique, nom, adresse physique et adresse IP au moment de l'enregistrement) et autres données telles que journaux de connexion IP, Xbox Gamertag et numéro de carte de crédit ou autres données de facturation, en réponse à un ordre/injonction à produire ;
- des données de contenu, y compris le contenu de courriers électroniques et de documents stockés sur OneDrive ou d'autres services sur le Cloud comme Office 365 ou Azure, en réponse à une ordonnance judiciaire ou un mandat.

Dans le cas des demandes provenant d'un pays autre que les États-Unis, Microsoft peut fournir directement les renseignements de base sur l'abonné (BSI) et les données transactionnelles sur réception d'une demande de son bureau en République d'Irlande.

[30] https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

Exemple de « renseignements de base sur l'abonné » fournis par Microsoft[31]

Le tableau ci-dessous montre ce que reçoit exactement un service de lutte contre la criminalité lorsque Microsoft produit les renseignements de base sur un abonné, en utilisant un compte de test enregistré par un employé de Microsoft. Nous avons modifié le nom et masqué le domaine pour des raisons de sécurité mais toutes les autres données sont exactement celles fournies par Microsoft.

Champ	Valeur
Login	Premier.Dernier@xxxxxxx.com
PUID	0006BFFDA0FF8810
Prénom	Premier
Nom de famille	Dernier
État	Washington
Code postal	98052
Pays	États-Unis
Fuseau horaire	Amérique/Los Angeles
Adresse IP d'enregistrement	65.55.161.10
Date d'enregistrement {Pacifique}	24.10.2007 13:05:18 PM
Sexe	M
Dernier IP de connexion	64.4.1.11

Dans le tableau ci-dessus, PUID désigne l'identifiant personnel de l'utilisateur (*Personal User ID*), qui est un code alphanumérique unique généré pour chaque compte enregistré par Microsoft.

Pour obtenir l'accès aux données de contenu, une requête d'entraide judiciaire est nécessaire.

L'équipe de conformité de Microsoft examine la demande, contrôle sa validité, la rejette si elle la juge non valide et communique uniquement les données spécifiées dans l'injonction légale.

Microsoft considère que la législation suivante s'applique aux données de ses clients :

- la loi ECPA (*Electronic Communication Privacy Act*) pour les données stockées aux États-Unis ;
- la législation irlandaise et les directives de l'Union européenne pour les comptes Hotmail et Outlook.com hébergés en Irlande ;
- la législation luxembourgeoise pour Skype qui est une filiale indépendante contrôlée à 100% par Microsoft et dont le siège se trouve au Luxembourg.

2.2.2.5 Twitter

Les demandes visant le contenu de communications (par ex. Tweets, messages directs, photos) doivent être accompagnées d'un mandat de perquisition ou document équivalent émis par un organe dont la juridiction s'applique effectivement à Twitter.

[31] https://www.microsoft.com/about/csr/transparencyhub/pppfaq/

Les services répressifs doivent adresser leurs demandes d'informations sur des comptes d'utilisateurs à Twitter Inc. (San Francisco, Californie) ou à Twitter International Company à Dublin (Irlande). Twitter répond aux demandes légales valides émises conformément à la législation applicable.

Les informations à caractère non public concernant des utilisateurs de Twitter ne peuvent être divulguées à un service répressif qu'en réponse à une procédure légale adéquate telle qu'une injonction, une ordonnance judiciaire ou une autre mesure légale valide – ou en réponse à une demande d'urgence valide.

Pour demander accès aux données de contenu, les services répressifs d'un pays autre que les États-Unis doivent adresser une requête d'entraide judiciaire aux autorités des États-Unis.

Les demandes d'informations relatives à un utilisateur doivent mentionner l'identifiant et l'URL du compte Twitter concerné, préciser les données spécifiques demandées et leur lien à une enquête en cours et être accompagnées d'une adresse de courrier électronique officielle. Ces demandes peuvent être soumises par télécopie ou courrier électronique sur format à en-tête du service répressif demandeur.

Twitter conserve différents types d'informations pendant des durées différentes, conformément à ses conditions d'utilisation et à sa politique de confidentialité. Certaines données (par ex. logs IP) ne sont conservées que pendant une période très brève. Les contenus supprimés par les utilisateurs de compte (par ex. Tweets) ne sont pas généralement accessibles.

2.2.2.6 Yahoo

Yahoo peut fournir en réponse aux demandes émanant des États-Unis :

- données de contenu, sur la base d'un mandat de perquisition ;
- renseignements de base sur l'abonné et données transactionnelles, sur la base d'une injonction ou d'une ordonnance judiciaire.

Yahoo déclare :

> Nous ne communiquons que les informations que nous sommes clairement obligés de produire dans une procédure légale, selon ce qu'autorise la loi. Nous résisterons à toute demande d'accès aux données de nos utilisateurs qui serait d'une ampleur injustifiée. Lorsque nous sommes tenus de fournir des informations, nous produisons seulement des données limitées pour satisfaire à la demande, afin de protéger la vie privée de nos utilisateurs[32].

Yahoo accepte généralement qu'une procédure légale lui soit notifiée par un organe gouvernemental des États-Unis par courrier électronique à l'adresse suivante : lawenforcement-request-delivery@yahoo-inc.com.

S'agissant des demandes émanant d'un pays autre que les États-Unis, Yahoo ne peut communiquer des données sur un utilisateur qu'à condition que la demande soit soumise via une requête d'entraide judiciaire. Yahoo ne répond pas aux demandes de données qui lui sont adressées directement par un service répressif étranger.

[32] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

Yahoo conserve différents types d'informations pendant des durées différentes. En général, les données de connexion d'un utilisateur pour la dernière année peuvent être fournies en réponse à une procédure légale. Les utilisateurs peuvent exercer un contrôle sur les contenus qu'ils stockent sur le réseau Yahoo et supprimer, altérer ou modifier ces contenus à tout moment. Les courriers électroniques définitivement supprimés ne peuvent être fournis en réponse à une procédure légale.

2.2.3 Demandes de conservation de données

2.2.3.1 Apple

Apple peut conserver des données sur demande reçue directement d'un service répressif étranger. Cependant, « toutes les données de contenu iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. Lorsqu'il fait appel à un autre fournisseur pour stocker des données, Apple ne lui communique en aucun cas les clés de chiffrement. Apple conserve ces clés dans ses centres de données aux États-Unis ». Par conséquent, les demandes de conservation de données doivent être envoyées à Apple Inc. et les contenus peuvent être obtenus uniquement via une requête d'entraide judiciaire.

De plus, en cas de demande de conservation d'une adresse électronique ou d'une adresse physique ou d'un numéro de téléphone concernant un identifiant/compte Apple, Apple n'extrait qu'une seule fois les données existantes sur l'utilisateur et conserve ces données pendant une période de 90 jours.

2.2.3.2 Facebook

Facebook accepte les demandes directes de conservation de données en relation avec une enquête pénale officielle et conserve les données pendant une période de 90 jours « en attendant la réception de l'action judiciaire formelle ». Les demandes doivent être soumises via le système de demande en ligne (*Law Enforcement Online Request System,* facebook.com/records) ou par courrier électronique ou postal ».

Facebook ne conserve pas les données mais s'efforce, en cas d'action judiciaire, de localiser et d'extraire les données non encore supprimées par les utilisateurs.

2.2.3.3 Google

En pratique, Google peut conserver des données sur demande directe d'un service répressif étranger. Une lettre signée envoyée par courrier électronique est requise.

La conservation des données peut être prolongée sur demande, en informant Google de l'envoi d'une lettre de demande (*letter of request, LOR*).

2.2.3.4 Microsoft

En pratique, Microsoft peut conserver des données sur demande directe d'un service répressif étranger. Microsoft exige l'envoi d'une lettre signée par télécopie.

Microsoft conserve les données initialement pour une période de 180 jours, qui peut ensuite être prolongée sur demande par périodes de 90 jours, en informant Microsoft de l'envoi d'une lettre de demande (*letter of request, LOR*).

Microsoft ne peut indiquer à un service répressif si un identifiant de compte est valide.

Les informations ci-dessus ne s'appliquent pas aux données conservées dans le Cloud.

2.2.3.5 Twitter

Twitter accepte les demandes directes de conservation de données reçues de services répressifs, en conservant un instantané temporaire des fichiers de compte pertinents pendant une période de 90 jours dans l'attente de la notification d'une mesure judiciaire valide.

> Les demandes de conservation doivent, conformément à la législation applicable, être signées par le représentant de l'organe requérant, mentionner le @nom d'utilisateur et l'URL du profil Twitter concerné (par ex. @safety et https://twitter.com/safety), inclure une adresse de retour officielle en état de validité et être envoyées sur papier à en-tête de l'organe demandeur[33].

2.2.3.6 Yahoo

> Nous conservons les données des utilisateurs, dans la mesure où elles sont disponibles, pendant une période de 90 jours sur réception d'une demande de conservation d'un organe gouvernemental valide et émise conformément à la législation applicable[34].

Les demandes de conservation reçues de services répressifs étrangers sont acceptées.

2.2.4 Procédures d'urgence

2.2.4.1 Apple

Dans le cas des demandes provenant de la région Europe/Moyen-Orient/Inde/Afrique, Apple considère une demande comme demande d'urgence s'il existe une « menace réelle grave pour : 1) la vie/sûreté d'un ou de plusieurs individus ; 2) la sécurité d'un État ; et 3) des infrastructures ou installations critiques avec un risque de dommages substantiels ».

Le formulaire suivant doit être utilisé pour les demandes d'urgence provenant de la région Europe/Moyen-Orient/Inde/Afrique : http://www.apple.com/legal/privacy/le-emergencyrequest.pdf

Avant de divulguer les données d'un client, Apple contacte le supérieur de l'agent demandeur pour confirmation du caractère légitime de la demande. Un agent demandeur peut aussi appeler un numéro spécial pour notifier Apple d'une demande urgente.

Apple informe le client de la demande de données dans un délai de 90 jours :

> Apple a pour politique de notifier le client dans un délai de 90 jours en cas de réception d'une demande urgente d'informations sur un compte client émanant d'un organe de lutte contre la criminalité.

2.2.4.2 Facebook

[33] https://support.twitter.com/articles/41949#
[34] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

> En cas d'affaire impliquant un danger imminent pour un enfant ou un risque de décès ou de blessures graves pour un individu et exigeant la divulgation d'informations sans délai, un agent des services répressifs peut soumettre une demande via le système de demande en ligne (*Law Enforcement Online Request System*) à : facebook.com/records.

2.2.4.3 Google

Google déclare au sujet des procédures d'urgence :

> Nous divulguons parfois volontairement des informations sur les utilisateurs à des organes gouvernementaux lorsque nous pensons que cela est nécessaire pour prévenir un décès ou des dommages physiques graves. La loi nous autorise à de telles exceptions, par exemple dans les affaires d'enlèvement ou de menace d'attentat. Les demandes d'urgence doivent inclure une description de l'urgence et expliquer de quelle façon les informations demandées pourraient empêcher les dommages. Nous ne fournissons en réponse à la demande que les informations qui nous semblent pouvoir aider à empêcher les dommages[35].

2.2.4.4 Microsoft

Microsoft a mis en place un programme pour la divulgation d'information en cas de demandes urgentes concernant un danger imminent.

Microsoft communique des informations aux organes de lutte contre la criminalité dans un nombre de cas limité, si :

> la divulgation d'information est nécessaire pour répondre à une situation d'urgence impliquant un danger de mort ou de blessures physiques graves pour un individu. Microsoft examine les demandes d'urgence reçues des services répressifs du monde entier. Ces demandes doivent être formulées par écrit sur papier à en-tête officiel et signées par une autorité judiciaire. Elles doivent décrire succinctement la situation d'urgence, en expliquant comment l'information recherchée aidera le service répressif à résoudre la situation. Chaque demande est soigneusement évaluée par l'équipe de conformité de Microsoft avant toute divulgation de données, et la divulgation se limite aux données qui nous semblent devoir permettre aux organes répressifs de résoudre la situation d'urgence. Les demandes d'urgence les plus fréquentes portent sur des menaces de suicide ou d'enlèvement[36].

2.2.4.5 Twitter

Twitter peut communiquer des informations sur un compte aux services répressifs en réponse à une demande valide de divulgation d'urgence.

Twitter indique qu'en cas de réception de demandes de données concernant une situation d'urgence :

> Nous évaluons les demandes de divulgation d'urgence au cas par cas, conformément à la législation pertinente [18 U.S.C. § 2702(b)(8) et article 8 de la loi irlandaise sur la protection des données, 1988 et 2003]. Dans le cas où nous recevrions des informations amenant raisonnablement à penser qu'il existe une situation d'urgence impérative réelle impliquant un

[35] https://www.google.com/transparencyreport/userdatarequests/legalprocess/
[36] https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/

danger de mort ou de blessures physiques graves pour une personne, nous pourrons décider de fournir l'information nécessaire pour prévenir ce danger, si nous disposons de cette information[37].

2.2.4.6 Yahoo

Conformément aux dispositions de la loi ECPA (18 U.S.C. § 2702) sur la divulgation urgente d'informations, nous communiquons des données aux représentants des pouvoirs publics lorsque nous avons reçu des informations permettant de conclure qu'une divulgation est nécessaire sans délai pour prévenir un danger imminent de mort ou de blessures physiques graves pour un individu. Toutes les demandes de divulgation d'urgence doivent être soumises par écrit en utilisant notre formulaire type. Yahoo détermine, à son entière discrétion, si les circonstances justifient la communication des données, sur la base des informations fournies dans le formulaire type de demande de divulgation d'urgence. Conformément à notre engagement de protéger la vie privée de nos utilisateurs et en vertu de la discrétion qu'autorise la loi ECPA, nous nous réservons le droit de communiquer uniquement les données que nous jugeons nécessaires pour éviter une situation d'urgence[38].

2.2.5 Notification du client

2.2.5.1 Apple

Apple notifie ses clients que leurs données personnelles font l'objet d'une demande d'information légalement valide de la part d'un service répressif, sauf s'il a des motifs raisonnables de penser qu'une telle notification risquerait de pervertir le cours de la justice ou de nuire à l'administration de la justice.

Apple notifie après-coup ses clients d'une demande d'information d'urgence, sauf s'il a des motifs raisonnables de penser qu'une telle notification risquerait de pervertir le cours de la justice ou de nuire à l'administration de la justice. Apple notifie ses clients d'une demande après expiration de la période de non-communication spécifiée dans une ordonnance judiciaire, sauf s'il a des motifs raisonnables de penser qu'une telle notification risquerait de pervertir le cours de la justice ou de nuire à l'administration de la justice.

Le formulaire type pour les demandes d'urgence[39] indique :

Apple a pour politique de notifier le client dans un délai de 90 jours en cas de réception d'une demande urgente d'informations sur un compte client émanant d'un organe de lutte contre la criminalité.

2.2.5.2 Facebook

Nous avons pour politique de notifier les utilisateurs de notre service des demandes d'accès à leurs données avant toute divulgation, sauf si la loi nous interdit de le faire ou dans certaines situations exceptionnelles, par exemple les affaires d'exploitation d'enfants et les situations d'urgence, ou lorsqu'une telle notification pourrait avoir un effet contraire au but recherché. Nous envoyons aussi une notification tardive à l'expiration de la période de non-communication spécifiée dans une ordonnance judiciaire ou lorsque nous pensons de bonne foi que les

[37] https://support.twitter.com/articles/41949#
[38] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm
[39] http://www.apple.com/legal/privacy/le-emergencyrequest.pdf

circonstances exceptionnelles ont cessé d'exister et que la loi ne nous interdit pas de le faire. Si un policier pense qu'une notification est de nature à nuire à une enquête, il doit obtenir une décision judiciaire adéquate ou toute autre mesure appropriée interdisant cette notification. Lorsqu'une demande de données attire notre attention sur une violation continue de nos conditions d'utilisation, nous prenons des mesures pour faire cesser cette violation, y compris en notifiant l'utilisateur que nous avons connaissance de son inconduite[40].

2.2.5.3 Google

Lorsqu'il reçoit une demande de données, Google notifie l'utilisateur par courrier électronique avant toute divulgation d'information, sauf s'il existe :

- un texte de loi, une décision judiciaire ou une autre contrainte légale ;
- des circonstances exceptionnelles impliquant un danger de mort ou de blessures physiques graves pour un individu ;
- une raison de penser que la notification ne parviendrait pas au détenteur effectif du compte, par exemple en cas de détournement de compte.

2.2.5.4 Microsoft

Lorsqu'il reçoit une demande de données, Microsoft notifie l'utilisateur par courrier électronique avant toute divulgation d'information, sauf dans les cas suivants :

- lorsque cela est interdit par la loi ;
- dans les cas d'urgence ;
- lorsque la notification pourrait être cause de danger ;
- lorsque la notification pourrait avoir un effet contraire au but recherché.

Cependant, même dans ces cas, Microsoft notifie tardivement l'utilisateur à expiration de l'ordonnance de non-communication valide et applicable, sauf s'il considère qu'une telle notification pourrait mettre en danger des individus ou aboutir à un effet contraire au but recherché.

2.2.5.5 Twitter

Twitter a pour politique de notifier les utilisateurs des demandes d'accès aux données de leur compte, en incluant une copie de la demande, avant la divulgation de ces données, sauf si la loi nous interdit de le faire [par ex. sous l'effet d'une ordonnance émise au titre de la loi 18 U.S.C. § 2705(b)], ainsi qu'en cas de circonstances impératives ou si une notification préalable risquerait d'avoir un effet non souhaité (par ex. situation d'urgence, compromission de comptes). Nous pouvons aussi notifier après-coup les utilisateurs concernés lorsqu'une notification préalable est interdite[41].

2.2.5.6 Yahoo

Nous avons pour politique de notifier expressément nos utilisateurs, avant toute divulgation, des demandes d'accès à leurs données qui émanent de tiers, en leur donnant ainsi la possibilité de contester ces demandes. Dans certains cas, la loi nous interdit de le faire, par exemple en cas de réception d'une ordonnance de non-communication émise au titre de la loi 18 U.S.C. § 2705(b).

[40] https://www.facebook.com/safety/groups/law/guidelines/
[41] https://support.twitter.com/articles/41949#

En outre, dans certaines circonstances exceptionnelles, par exemple une menace imminente de dommages physiques pour un individu, nous pouvons choisir de retarder l'envoi de la notification. Lorsque les circonstances qui ont empêché la notification préalable de l'utilisateur avant la divulgation de données cessent d'exister, par exemple du fait de l'expiration d'une ordonnance de non-communication ou de l'extinction de la menace, nous prenons des mesures pour informer le ou les utilisateurs concernés de la divulgation de données[42].

2.3 Accords entre services répressifs et fournisseurs de services

Dans plusieurs Parties à la Convention, les autorités ont conclu des accords ou pris des dispositions pour améliorer la coopération avec les fournisseurs de services basés aux États-Unis, notamment en convenant de l'utilisation de formulaires types pour les demandes d'information, en définissant les procédures à suivre et en établissant des points de contact uniques. Cela est notamment le cas en France et au Portugal.

Dans les Parties à la Convention où ont été établis de tels accords, un plus grand nombre de demandes sont envoyées et le nombre des informations reçues est aussi plus élevé. Les autorités de justice pénale et les fournisseurs de services soulignent conjointement que ces bonnes pratiques ont un impact réel[43].

3 Les aspects problématiques[44]

La divulgation volontaire par les fournisseurs de services basés aux États-Unis d'informations relatives aux abonnés est extrêmement utile aux autorités de justice pénale dans les Parties à la Convention de Budapest. Néanmoins, un certain nombre de problèmes et de préoccupations ont été soulevés à cet égard.

3.1 Volatilité des politiques des fournisseurs de services

Les politiques des fournisseurs de services sont volatiles et manquent de prévisibilité pour les organes répressifs[45] ainsi que pour les clients. Les fournisseurs de services peuvent modifier leurs politiques de façon unilatérale à tout moment, sans en notifier préalablement les organes répressifs[46].

[42] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

[43] Voir aussi les *Lignes directrices pour la coopération entre organes répressifs et fournisseurs de services internet contre la cybercriminalité*, développées en 2008, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba

[44] Ces différents problèmes ont été soulevés par les services répressifs et les fournisseurs de services au cours de l'audition du 30 novembre 2015. Les règles de Chatham House ayant été acceptées, ils ne peuvent être attribués à un fournisseur ou à un service répressif particulier.

[45] Voir, par exemple, la situation italienne en 2006-2008 (les filiales de Google, Microsoft et Yahoo étant toutes basées à Milan), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2625 :
Microsoft Italia a été le premier à fournir – sans commission rogatoire, sur simple demande du ministère public italien – des informations relatives aux abonnés, non seulement pour les comptes *hotmail.it* mais aussi pour les comptes de courrier électronique *hotmail.com*.
Dans un premier temps, Google Italia a mis en avant la nécessité d'une procédure d'entraide judiciaire pour toute demande de données. Puis, après l'affaire Google Italia, ce fournisseur a modifié sa politique et commencé à fournir directement des informations relatives aux abonnés en exigeant une ordonnance du ministère public italien (et pas seulement un ordre de la police judiciaire italienne). Néanmoins, dans les cas où une adresse IP (enregistrée par les systèmes électroniques de Google pour un courrier de type *@gmail.com*) ne se rapportait pas à un serveur italien, Google se considérait dans l'incapacité de la communiquer à l'autorité judiciaire italienne.
Yahoo! Italia, en revanche, n'exigeait une commission rogatoire que dans certains cas, ayant mis en place un logiciel appelé *Yahoo! Account Management Tool* qui pouvait récupérer aussi les données de contenu sur demande (spécifiquement les données des comptes de courrier électronique @*yahoo.it* et/ou @*yahoo.com*) mais seulement pour les utilisateurs ayant choisi au moment de leur inscription d'être soumis à la législation italienne (selon le

En outre, les politiques et les pratiques non seulement diffèrent largement entre fournisseurs mais aussi au regard des différentes Parties à la Convention de Budapest. Un fournisseur peut répondre positivement à de nombreuses demandes d'un pays et à aucune ou très peu d'un autre – et un autre fournisseur peut avoir des pratiques exactement inverses.

D'une manière générale, les politiques et les pratiques des fournisseurs sont volatiles et imprévisibles, ce qui est problématique du point de vue de l'état de droit.

3.2 Localisation

Les problèmes de localisation, de territorialité et de compétence ont été décrits dans le document de travail intitulé « Criminal justice access to data in the cloud : challenges »[47].

Dans la coopération entre les fournisseurs de services basés aux États-Unis et les services répressifs d'autres Parties, il semblerait que la localisation effective des données ou des serveurs n'ait qu'une pertinence réduite pour ce qui concerne les demandes de renseignements sur des abonnés. Les conditions d'accès aux renseignements sur des abonnés semblent déterminées par : (a) la localisation du fournisseur de services et la réglementation à laquelle il est soumis ; et (b) la question de savoir si l'autorité judiciaire requérante est compétente pour traiter l'infraction en cause. Les fournisseurs de services basés aux États-Unis divulguent en général aux services répressifs, sous certaines conditions, des données relatives aux abonnés dans les pays où ils gèrent un service, comme prévu à l'article 18.1.b de la Convention de Budapest.

Les fournisseurs de services européens semblent être liés par des règles de territorialité, notamment au sujet de la localisation des données. L'audition du 30 novembre 2015[48] a montré que, pour les fournisseurs européens, cela constitue un obstacle majeur à leurs activités.

En ce qui concerne les données de contenu, la position des fournisseurs des États-Unis n'est pas claire. Dans certains cas, ils font valoir que, ces données étant stockées aux États-Unis, il ne leur est pas possible de les divulguer volontairement (sauf dans les situations d'urgence) – alors que, dans d'autres cas où les données sont stockées en Europe, ils continuent à exiger l'envoi d'une demande d'entraide judiciaire au gouvernement des États-Unis.

3.3 Fournisseurs « américains » et fournisseurs « européens » ou autres

Les fournisseurs de services basés aux États-Unis peuvent communiquer directement et volontairement, sur demande, des données sur les abonnés et le trafic à des services étrangers de lutte contre la criminalité. Ils peuvent aussi fournir des données de contenu dans les situations

principe de « citoyenneté du Net »). Yahoo! Italia pouvait aussi fournir des courriers interceptés aux autorités judiciaires italiennes (sans qu'une procédure d'entraide judiciaire soit nécessaire).
Yahoo!, bien que divulguant directement aussi des données de contenu aux autorités judiciaires italiennes, refusait pendant les mêmes années de divulguer quoi que ce soit aux autorités judiciaires belges (voir l'affaire Yahoo! en Belgique).

[46] *Apple Legal Process Guidelines*, version du 29 septembre 2015 : « Rien dans ces lignes directrices ne peut être interprété comme créant des droits exécutoires au regard d'Apple et les politiques d'Apple pourront être mises à jour ou modifiées à l'avenir sans autre notification des organes répressifs ».

[47] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

[48] http://www.coe.int/en/web/cybercrime/hearing

d'urgence. Cela est autorisé par la législation des États-Unis (*Electronic Communications Privacy Act*)[49].

Il semblerait que les fournisseurs de services européens ne divulguent pas directement des données aux autorités étrangères et répondent uniquement aux ordonnances émises par les autorités nationales suite à une requête d'entraide judiciaire.

Les raisons de cette situation ne sont pas tout à fait claires. Alors que les fournisseurs de « services de communication électronique » en Europe sont normalement soumis à des normes strictes en ce qui concerne la divulgation des données de trafic, les fournisseurs de « services internet et de la société de l'information » doivent en principe être en mesure de divulguer des renseignements sur les abonnés sur la base de motifs légitimes, urgents ou d'intérêt public.

Il en résulte un flux de données à sens unique des fournisseurs de services basés aux États-Unis vers les services répressifs des Parties à la Convention en Europe et d'autres régions, les fournisseurs de services des pays européens ou d'autres Parties ne communiquant pas directement et volontairement des données aux autorités des États-Unis ou d'autres Parties à la Convention.

Les fournisseurs de services des États-Unis sont de plus en plus présents à l'intérieur de l'Union européenne – par l'intermédiaire de filiales en Irlande par exemple – et sont donc soumis au droit de l'Union européenne et, en particulier, à la réglementation sur la protection des données. Cela pourrait restreindre à l'avenir les possibilités de coopération transfrontière directe et volontaire.

D'autre part, on peut se demander pourquoi ce qui est possible pour les fournisseurs de services basés aux États-Unis présents directement ou indirectement dans l'Union européenne – à savoir la divulgation volontaire d'informations relatives aux abonnés et, dans les situations d'urgence, d'autres données également – n'est pas possible pour les fournisseurs de services européens.

3.4 Base légale existant dans le droit interne pour l'obtention de données relatives à un abonné

Les fournisseurs de services basés aux États-Unis, lorsqu'ils reçoivent une demande de données d'un service répressif étranger, examinent le cadre légal interne auquel est soumis l'organe requérant et, en particulier, la question de savoir si cet organe dispose effectivement du pouvoir de requérir certaines données des fournisseurs de services à l'échelon national.

Comme indiqué dans le rapport du T-CY sur les conditions requises pour l'obtention de données relatives à un abonné[50], les conditions d'accès à ces données varient entre les Parties à la Convention. Dans certaines, les policiers et, dans d'autres, les procureurs peuvent exiger la production de données sur des abonnés, tandis que, dans d'autres, une ordonnance judiciaire est requise. Dans ce dernier cas, les fournisseurs de services peuvent décider d'ignorer une demande de la police ou d'une autorité de poursuite.

Dans certaines Parties, une distinction est faite entre l'information sur les abonnés (et d'autres données) détenue par les fournisseurs de services de télécommunications et l'information détenue par les fournisseurs de services internet et de la société de l'information. Étant donné la convergence

[49] 18 U.S. Code § 2702, https://www.law.cornell.edu/uscode/text/18/2702
[50] T-CY (2014)17, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

entre les différents types de services et de fournisseurs de services, cette distinction devient en pratique de plus en plus problématique.

L'absence d'harmonisation des règles sur l'obtention des données relatives à un abonné dans les Parties à la Convention de Budapest complique les choses pour les fournisseurs de services qui sont prêts à coopérer.

Une autre question concerne la recevabilité de l'information fournie volontairement par un fournisseur de services étranger comme élément de preuve dans une procédure pénale. Dans certaines Parties, cette information est recevable, dans d'autres non.

Cela montre que l'existence dans le droit interne d'une base légale claire pour l'obtention des données relatives à un abonné, de préférence harmonisée entre les Parties, permettrait une coopération plus systématique avec les fournisseurs de juridictions étrangères et faciliterait l'utilisation de l'information reçue dans les procédures pénales.

3.5 Demandes de conservation de données adressées directement à un fournisseur de services

Les fournisseurs de services basés aux États-Unis acceptent les demandes de conservation reçues directement d'autorités étrangères. Toutefois, l'absence fréquente de suivi de ces demandes au moyen d'une demande d'entraide judiciaire est pour eux cause de préoccupation.

Les fournisseurs européens n'acceptent pas les demandes de conservation reçues directement de services répressifs d'autres juridictions.

3.6 Demandes d'urgence

Les fournisseurs de services basés aux États-Unis ont prévu la mise en œuvre de procédures de coopération dans les situations d'urgence, y compris la divulgation de contenus.

Dans certaines Parties à la Convention, des procédures spécifiques ont été établies, en particulier la mise en place de systèmes centralisés et de points de contact. Dans ces Parties, l'expérience semble globalement positive, bien que la coopération avec certains fournisseurs de services ne soit pas toujours considérée comme prévisible ou fiable, y compris dans les situations d'urgence.

Alors que les fournisseurs de services basés aux États-Unis coopèrent en principe effectivement dans les situations d'urgence, Il semblerait que les fournisseurs de services européens ne communiquent pas directement d'informations sur les abonnés ou d'autres données aux autorités étrangères, même dans les situations d'urgence.

3.7 Notification du client

La notification du client par les fournisseurs de services basés aux États-Unis en cas de demande d'une autorité étrangère est un sujet de préoccupation majeur pour les services répressifs.

Le respect des règles de confidentialité peut être assuré dans les procédures légales de demande de données au niveau national, mais cela n'est pas autant le cas dans les situations de coopération volontaire avec un fournisseur de services étranger.

Notification du client : exemple communiqué par un procureur d'un État Partie à la Convention de Budapest (novembre 2015)

1. Nous lisons sur [COMPTE DE MEDIA SOCIAL] que quelqu'un écrivant au nom d'ISIS annonce que [VILLE] sera attaquée le [DATE]
2. Nous trouvons également cette information sur [COMPTE DE MEDIA SOCIAL]
3. [LE FOURNISSEUR DE MEDIA SOCIAL] nous communique, sur la base d'une demande d'urgence, les données relatives à l'abonné et son identifiant de connexion. Jusqu'ici les choses se déroulent normalement.
4. Nous voyons qu'un compte [WEBMAIL] est connecté au [COMPTE DE MEDIA SOCIAL].
5. Pour obtenir plus d'informations, nous adressons une demande similaire au [FOURNISSEUR DE WEBMAIL].
6. Celui-ci nous communique sa nouvelle politique dans laquelle il est indiqué clairement que, même en cas de procédure concernant une menace physique imminente, il se réserve le droit de notifier le client.
7. Nous demandons des précisions : « QUESTION AU SUJET DE LA POLITIQUE DE DIVULGATION DU [FOURNISSEUR DE WEBMAIL] : QUELLES INFORMATIONS SUR LE DEMANDEUR FOURNIREZ-VOUS AU DÉTENTEUR DU COMPTE ? S'AGIRA-T-IL D'INDICATIONS ASSEZ GÉNÉRALES COMME "LES AUTORITÉS DE [PAYS]" OU ALLEZ-VOUS DIVULGUER LE NOM ET L'ADRESSE DE COURRIER ÉLECTRONIQUE DE LA PERSONNE QUI A SIGNÉ LA DEMANDE DE DIVULGATION D'URGENCE ? NOUS SOUHAITONS OBTENIR UNE RÉPONSE À CE SUJET CAR, DANS LA SECONDE ÉVENTUALITÉ, UN TERRORISTE POTENTIEL POURRAIT RECEVOIR DES INFORMATIONS À CARACTÈRE PERSONNEL SUR UN AGENT DES SERVICES JUDICIAIRES ».
8. Le fournisseur de Webmail nous a rappelé en déclarant comprendre la situation mais en disant qu'il ne pouvait garantir qu'au bout de 90 jours ces informations personnelles ne seraient pas communiquées au client.

3.8 Protection des données

Plus les fournisseurs des États-Unis seront présents en Europe, plus ils seront soumis aux normes européennes de protection des données.

Les instruments européens et internationaux de protection des données couvrent les transferts de données transfrontières d'une entité du secteur privé vers une autre entité du secteur privé ou d'une autorité de justice pénale compétente vers une autre autorité de justice pénale.

Le transfert « asymétrique » de données d'une autorité de justice pénale compétente d'un État membre de l'UE à des personnes privées d'un autre État membre est autorisé sous certaines conditions spécifiques[51].

Cependant, il ne semble pas exister de règles claires autorisant la divulgation volontaire « asymétrique » de données – telles que les données relatives à un abonné – d'un fournisseur de services du secteur privé à une autorité judiciaire d'un autre État.

Les fournisseurs de services doivent évaluer eux-mêmes si les conditions de légalité sont remplies, c'est-à-dire s'il est dans l'intérêt public ou dans l'intérêt légitime du fournisseur en tant que maître du

[51] Article 14 de la Décision cadre 2008/977/JAI, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN, et article 36 aa du projet de future directive de l'UE sur la protection des données dans le secteur de la justice pénale, http://statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft-final-compromise-15174-15.pdf

fichier de divulguer les données. Les fournisseurs sont donc exposés au risque d'être tenus pour responsables. Un cadre plus clair pour la divulgation transfrontière de données du secteur privé vers une autorité publique, incluant des conditions et des sauvegardes, est donc nécessaire. Un tel cadre éviterait aux fournisseurs de services de se trouver face à des obligations légales contradictoires.

Exemple : audit de Facebook Ireland par le Commissaire irlandais à la protection des données 2011-2012

En 2011 et 2012, le Commissaire irlandais à la protection des données a réalisé un audit de Facebook Ireland, notamment en ce qui concerne la divulgation de données à des autorités étrangères[52].

La base légale autorisant Facebook à divulguer des données à des autorités de justice pénale est l'article 8 de la loi irlandaise sur la protection des données qui stipule que « les restrictions prévues dans cette loi au retard du traitement des données à caractère personnel ne s'appliquent pas » si, en particulier, le traitement est nécessaire dans un but de prévention de la criminalité ou aux fins de la justice pénale. Les dispositions 8(b) et 8(d) sont considérées comme spécialement pertinentes à cet égard :

8.- Les restrictions prévues dans cette loi au retard du traitement des données à caractère personnel ne s'appliquent pas si le traitement est :

> *(b) requis aux fins de la prévention, de la détection ou de l'investigation d'infractions, de l'appréhension ou de la poursuite d'auteurs d'infractions, ou de l'évaluation ou de la collecte de tout impôt, droit ou montant dû ou payable à l'État, une autorité locale ou un organe de santé, dans les cas où l'application de ces restrictions risquerait de nuire aux objectifs susmentionnés ;*
>
> *(d) nécessaire d'urgence pour empêcher des blessures ou tout autre atteinte à la santé d'un individu, une perte importante de biens ou l'endommagement de biens*.

Le service spécialisé (*Law enforcement unit*) de Facebook Ireland évalue donc si ces conditions sont remplies avant de répondre à une demande. « Chaque demande est examinée en tenant compte de l'autorité légale de l'organe répressif requérant et de la nature des données à caractère personnel demandées »[53].

Un aspect important de la procédure est que Facebook Ireland coopère avec les points de contact uniques (PCU) désignés au sein des services répressifs. « L'intérêt de cette approche est qu'elle réduit au minimum le risque de demandes inappropriées de données »[54].

En outre, « la base légale mentionnée dans chaque demande est examinée sous l'angle de la compatibilité avec la législation applicable et, en cas de doute, on sollicite également l'avis d'un juriste interne ou externe »[55].

[52] Voir section 3.7 (p. 98 et suiv.) et annexe 5 du rapport de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf ; voir section 2.7 (p. 34 et suiv.) du rapport de 2012, https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm
[53] Voir p. 99 du Rapport d'audit de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[54] Voir p. 99 du Rapport d'audit de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

La procédure suivie par Facebook a fait l'objet d'un audit en 2011[56] et 2012. Le rapport d'audit de 2011 examine cinq demandes étrangères (Royaume-Uni, Italie, Belgique, Allemagne et Italie) sélectionnées de manière aléatoire afin de déterminer si les critères établis aux articles 8(b) et 8(d) de la loi irlandaise sur la protection des données ont été respectés. En 2012, cinq autres demandes (France, Allemagne, Italie, Portugal, Royaume-Uni et Irlande) ont été examinées. Facebook a rejeté certaines demandes et répondu de manière positive à d'autres. L'échantillon couvrait uniquement des États membres de l'UE.

Les auditeurs ont jugé que les procédures et pratiques de Facebook en matière de divulgation de données à des autorités étrangères étaient conformes à la loi irlandaise sur la protection des données et considéré que les articles 8(b) et 8(d) constituaient une base légale suffisante.

Cet avis est intéressant puisque les États de l'UE et d'autres Parties à la Convention 108 sont normalement dotés de dispositions similaires dans leur législation nationale sur la protection des données. Si ces dispositions étaient interprétées de la même façon, les fournisseurs de services de ces pays devraient aussi être en mesure de divulguer des données aux autorités étrangères.

Pour l'accès aux contenus, une demande d'entraide juridique doit être envoyée aux autorités irlandaises :

« Lorsqu'un organe judiciaire demande à Facebook Ireland (FB-I) la divulgation de données de contenu, nous exigeons la production d'une requête légalement contraignante aux termes du droit irlandais. La Gardaí (police irlandaise) doit donc émettre un mandat de perquisition ou un autre document contraignant de même nature. FB-I ne pourra obtempérer à un mandat de perquisition émis par un organe non irlandais que si celui-ci est exécutoire en vertu du droit irlandais. Tout document de ce type devra donc être transposé dans le droit interne via le dépôt d'une demande d'entraide judiciaire au ministère de la justice, conformément à la loi de 2008 sur l'entraide judiciaire en matière pénale »[57].

3.9 Demandes légales ou coopération volontaire ?

Un ordre légal de la police, d'un procureur ou d'un juge adressé à une personne physique ou morale est contraignant et peut être exécuté sur le territoire de l'autorité concernée.

Néanmoins, dans leur pratique actuelle de coopération transfrontière directe, les fournisseurs de services basés aux États-Unis considèrent leur coopération comme « volontaire ».

La pratique actuelle combine donc demandes légales coercitives et coopération volontaire.

Les fournisseurs de services basés aux États-Unis semblent souhaiter maintenir les choses en l'état.

[55] Voir p. 99 du Rapport d'audit de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[56] Voir section 3.7 (p. 98 et suiv.) et annexe 5 du rapport de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf ; voir section 2.7 (p. 34 et suiv.) du rapport de 2012, https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm
[57] Voir p. 99 du Rapport d'audit de 2011, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

Cela paraît problématique du point de vue de l'application de la loi puisque ce sont les fournisseurs de services qui décident eux-mêmes de coopérer ou non, qui évaluent la légalité des demandes ou qui vérifient l'existence de la double incrimination et d'autres critères. Cela est vrai non seulement pour les demandes de données de données reçues de la police mais aussi pour celles reçues des procureurs et des tribunaux ; en définitive, les demandes ne sont pas exécutoires[58]. Les fournisseurs de services semblent donc au-dessus de la loi et cela est problématique du point de vue de l'état de droit.

4 Conclusions

La Cour européenne des droits de l'homme, dans l'arrêt *K. U. c. Finlande*[59] rendu en décembre 2008, souligne l'obligation pour les États de protéger les droits des individus, y compris au moyen de mesures de droit pénal efficaces. Dans son analyse, la Cour mentionne les dispositions de droit procédural de la Convention de Budapest sur la cybercriminalité, notamment l'article 18 sur la production des données relatives aux abonnés. Elle signale aussi le besoin d'une coopération efficace entre les fournisseurs de services et les services répressifs, comme proposé dans les lignes directrices adoptées par la Conférence Octopus du Conseil de l'Europe en avril 2008[60].

La coopération entre fournisseurs de services et services répressifs est donc essentielle aux fins de la prévention de la criminalité et de la justice pénale, ainsi que du renforcement de l'état de droit et de la protection des droits de l'homme.

Les fournisseurs de services basés aux États-Unis coopèrent souvent directement à travers les frontières avec les services répressifs d'autres Parties à la Convention de Budapest, en particulier en divulguant des informations relatives aux abonnés. Ceci est, par bien des aspects, conforme à l'article 18.1.b de la Convention de Budapest.

Dans ce type de situation, un fournisseur de services détenant ou contrôlant les données coopère avec un organe répressif compétent au regard de l'infraction spécifique donnant lieu à enquête. La localisation effective des données et des serveurs n'a qu'une pertinence limitée.

Les Parties à la Convention de Budapest – États-Unis non inclus – envoient plus de 100 000 demandes par an aux grands fournisseurs de services basés aux États-Unis et reçoivent des données (au moins partielles) dans 60% des cas.

Cette pratique des fournisseurs de services basés aux États-Unis est extrêmement utile aux fins de la prévention de la criminalité et de la justice pénale.

Cependant, étant volatile et imprévisible, elle soulève un certain nombre de préoccupations du point de vue de la protection des données et de la prééminence du droit.

Les fournisseurs de services européens et la plupart des fournisseurs non basés aux États-Unis ne coopèrent pas normalement de façon directe avec des services répressifs étrangers et paraissent plus fortement soumis aux règles de territorialité (localisation du maître des fichiers et localisation des données).

[58] Voir à ce sujet l'arrêt final de la Cour de cassation belge confirmant l'obligation pour Yahoo! de produire des données en réponse à une demande légale d'information en Belgique, http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f
[59] http://hudoc.echr.coe.int/eng#{"dmdocnumber":["843777"],"itemid":["001-89964"]}
[60] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba

La distinction entre fournisseurs de services de communications électroniques et fournisseurs de services internet et de la société de l'information complique encore les choses dans un contexte où un même fournisseur offre parfois différents types de services[61].

En conclusion, une politique commune en matière de divulgation pour tous les types de fournisseurs serait souhaitable.

La poursuite du dialogue avec les fournisseurs de services est nécessaire. La tenue de réunions régulières entre le T-CY et les fournisseurs de services, la création d'un outil en ligne donnant accès à des renseignements actualisés sur les politiques et les procédures des fournisseurs de services, ainsi qu'à des informations sur la législation pertinente et les autorités de justice pénale responsables dans les Parties à la Convention, et l'établissement de formulaires types communs pour les demandes de données relatives aux abonnés pourraient contribuer à améliorer les pratiques actuelles des Parties à la Convention de Budapest.

Toutefois, il ne sera pas seulement nécessaire d'améliorer les pratiques ; il faudra aussi établir des cadres juridiques nationaux et internationaux clairs pour parvenir à une plus grande sécurité juridique, tant pour les organes répressifs que pour les entités du secteur, et supprimer les obstacles existants pour les entreprises[62]. Ces dispositifs devront s'articuler autour de l'article 18 de la Convention de Budapest et/ou des dispositions d'un Protocole additionnel à la Convention.

[61] L'Union européenne semble s'acheminer vers une révision de la Directive 2002/58/CE (Directive vie privée et communications électroniques). Il est notamment proposé de supprimer la distinction entre fournisseurs de services de communications électroniques et fournisseurs de services internet et de la société de l'information ; https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

[62] Telle était aussi la conclusion de l'audition pour les fournisseurs de service organisée le 30 novembre 2015, http://www.coe.int/en/web/cybercrime/hearing

5 Annexe

5.1 Demandes directes adressées aux grands fournisseurs de services par des Parties à la Convention en 2014

2014	All providers			Requests share/all parties	Google and You Tube			Microsoft and Skype			Yahoo		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Albania	24	7	29%	0,01%	2	-	0%	-	-	0%	1	-	0%
Armenia	11	2	18%	0,01%	1	-	0%	4	1	25%	1	-	0%
Australia	6 438	4 236	66%	3,40%	1 711	1 014	59%	2 332	1 845	79%	769	395	51%
Austria	246	73	30%	0,13%	71	19	27%	51	29	57%	5	-	0%
Azerbaijan	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Belgium	1 804	1 316	73%	0,95%	427	299	70%	914	754	82%	5	-	0%
Bosnia and Herzegovina	13	8	62%	0,01%	1	-	0%	1	-	0%	-	-	0%
Bulgaria	5	3	60%	0,00%	1	-	0%	-	-	0%	-	-	0%
Canada	850	477	56%	0,45%	71	29	40%	129	104	81%	25	11	44%
Croatia	45	34	76%	0,02%	3	-	0%	2	2	100%	-	-	0%
Cyprus	38	21	55%	0,02%	-	-	0%	5	-	0%	-	-	0%
Czech Republic	333	204	61%	0,18%	216	115	53%	83	74	89%	-	-	0%
Denmark	362	225	62%	0,19%	119	62	52%	178	142	80%	5	-	0%
Dominican Republic	54	30	56%	0,03%	2	-	0%	19	18	95%	-	-	0%
Estonia	35	19	54%	0,02%	8	3	38%	14	9	64%	-	-	0%
Finland	144	102	71%	0,08%	35	29	83%	62	48	77%	1	-	0%
France	21 772	12 863	59%	11,49%	6 075	3 523	58%	8 766	7 007	80%	2 377	721	30%
Georgia	1	-	0%	0,00%	-	-	0%	-	-	0%	-	-	0%
Germany	25 519	13 801	54%	13,46%	6 452	3 252	38%	9 375	7 397	79%	4 786	1 467	31%
Hungary	345	159	46%	0,18%	38	-	0%	115	96	83%	7	-	0%
Iceland	3	2	67%	0,00%	-	-	0%	1	1	100%	-	-	0%
Italy	9 365	4 620	49%	4,94%	2 022	888	44%	1 769	1 242	70%	1 879	687	37%
Japan	1 617	1 010	62%	0,85%	252	199	79%	737	586	80%	-	-	0%

2014	All providers			Requests share/all parties	Google and You Tube			Microsoft and Skype			Yahoo		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Latvia	2	2	100%	0,00%	-	-	0%	2	2	100%	-	-	0%
Lichtenstein	5	1	20%	0,00%	2	-	0%	-	-	0%	-	-	0%
Lithuania	49	28	57%	0,03%	12	9	75%	15	10	67%	1	-	0%
Luxembourg	153	117	76%	0,08%	1	-	0%	138	111	80%	-	-	0%
Malta	377	197	52%	0,20%	99	57	58%	90	71	79%	9	-	0%
Mauritius	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Moldova	13	7	54%	0,01%	1	-	0%	5	3	60%	-	-	0%
Montenegro	7	1	14%	0,00%	-	-	0%	1	-	0%	-	-	0%
Netherlands	1 099	856	78%	0,58%	212	172	81%	734	607	83%	16	-	0%
Norway	363	238	66%	0,19%	93	48	52%	203	167	82%	12	-	0%
Panama	88	68	77%	0,05%	-	-	0%	88	68	77%	-	-	0%
Poland	1 747	550	31%	0,92%	1 046	307	29%	103	72	70%	1	-	0%
Portugal	2 223	1 356	61%	1,17%	647	346	53%	897	760	85%	18	-	0%
Romania	80	40	50%	0,04%	49	26	53%	-	-	0%	1	-	0%
Serbia	16	9	56%	0,01%	1	-	0%	-	-	0%	-	-	0%
Slovakia	107	36	34%	0,06%	62	5	8%	37	30	81%	3	-	0%
Slovenia	11	6	55%	0,01%	5	3	60%	2	2	100%	1	-	0%
Spain	4 462	2 391	54%	2,35%	1 394	690	50%	1 484	1 192	80%	429	114	27%
Sri Lanka	1	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Switzerland	462	266	58%	0,24%	254	169	66%	110	81	74%	12	-	0%
The former Yugoslav Republic of Macedonia	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Turkey	8 405	5 625	67%	4,43%	568	-	0%	7 130	5 411	76%	-	-	0%
Ukraine	8	2	25%	0,00%	5	1	20%	2	1	50%	-	-	0%
United Kingdom	20 127	13 894	69%	10,62%	3 615	2 665	74%	8 608	6 602	77%	2 978	1 141	38%
USA	80 703	63 147	78%	42,58%	22 520	18 318	81%	12 364	8 062	65%	11 656	9 680	83%
Total excl. USA	**108 829**	**64 901**	**60%**		**25 573**	**13 930**	**54%**	**44 206**	**34 545**	**78%**	**13 342**	**4 536**	**34%**
Total incl. USA	**189 532**	**128 048**	**68%**	**100%**	**48 093**	**32 248**	**67%**	**56 570**	**42 607**	**75%**	**24 998**	**14 216**	**57%**

2014	All providers			Requests share/all parties	Facebook			Twitter			Apple		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Albania	24	7	29%	0,01%	20	7	35%	1	-	0%	-	-	0%
Armenia	11	2	18%	0,01%	5	1	20%	-	-	0%	-	-	0%
Australia	6 438	4 236	66%	3,40%	1 439	937	65%	12	7	58%	175,0	37,6	21%
Austria	246	73	30%	0,13%	109	16	15%	-	-	0%	10,0	9,0	90%
Azerbaijan	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Belgium	1 804	1 316	73%	0,95%	448	260	58%	1	-	0%	9,0	3,0	33%
Bosnia and Herzegovina	13	8	62%	0,01%	11	8	73%	-	-	0%	-	-	0%
Bulgaria	5	3	60%	0,00%	3	3	100%	-	-	0%	1,0	-	0%
Canada	850	477	56%	0,45%	542	303	56%	62	18	29%	21,0	13,0	62%
Croatia	45	34	76%	0,02%	40	32	80%	-	-	0%	-	-	0%
Cyprus	38	21	55%	0,02%	33	21	64%	-	-	0%	-	-	0%
Czech Republic	333	204	61%	0,18%	33	15	45%	-	-	0%	1,0	-	0%
Denmark	362	225	62%	0,19%	46	17	37%	4	1	25%	10,0	3,0	30%
Dominican Republic	54	30	56%	0,03%	33	12	36%	-	-	0%	-	-	0%
Estonia	35	19	54%	0,02%	13	7	54%	-	-	0%	-	-	0%
Finland	144	102	71%	0,08%	46	25	54%	-	-	0%	-	-	0%
France	21 772	12 863	59%	11,49%	4 343	1 568	36%	96	11	11%	115,0	33,0	29%
Georgia	1	-	0%	0,00%	1	-	0%	-	-	0%	-	-	0%
Germany	25 519	13 801	54%	13,46%	4 669	1 592	34%	31	5	16%	206,0	87,7	43%
Hungary	345	159	46%	0,18%	185	63	34%	-	-	0%	-	-	0%
Iceland	3	2	67%	0,00%	2	1	50%	-	-	0%	-	-	0%
Italy	9 365	4 620	49%	4,94%	3 643	1 784	49%	10	2	20%	42,0	17,0	41%
Japan	1 617	1 010	62%	0,85%	11	1	9%	480	173	36%	137,0	51,0	37%
Latvia	2	2	100%	0,00%	-	-		-	-	0%	-	-	0%
Lichtenstein	5	1	20%	0,00%	3	1	33%	-	-		-	-	
Lithuania	49	28	57%	0,03%	20	9	45%	1	-	0%	-	-	0%
Luxembourg	153	117	76%	0,08%	5	2	40%	-	-	0%	9,0	4,0	44%

2014	All providers			Requests share/all parties	Facebook			Twitter			Apple		
Parties	**Received**	**Disclosure**	**%**		**Received**	**Disclosure**	**%**	**Received**	**Disclosure**	**%**	**Received**	**Disclosure**	**%**
Malta	377	197	52%	0,20%	178	68	38%	-	-	0%	1,0	1,0	100%
Mauritius	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Moldova	13	7	54%	0,01%	7	4	57%	-	-	0%	-	-	0%
Montenegro	7	1	14%	0,00%	6	1	17%	-	-	0%	-	-	0%
Netherlands	1 099	856	78%	0,58%	117	72	62%	9	2	22%	11,0	3,0	27%
Norway	363	238	66%	0,19%	46	20	43%	2	1	50%	7,0	2,0	29%
Panama	88	68	77%	0,05%	-	-		-	-	0%	-	-	0%
Poland	1 747	550	31%	0,92%	593	169	28%	-	-	0%	4,0	2,0	50%
Portugal	2 223	1 356	61%	1,17%	659	249	38%	1	-	0%	1,0	1,0	100%
Romania	80	40	50%	0,04%	30	14	47%	-	-	0%	-	-	0%
Serbia	16	9	56%	0,01%	15	9	60%	-	-	0%	-	-	0%
Slovakia	107	36	34%	0,06%	5	1	20%	-	-	0%	-	-	0%
Slovenia	11	6	55%	0,01%	3	1	33%	-	-	0%	-	-	0%
Spain	4 462	2 391	54%	2,35%	1 014	373	37%	112	13	12%	29,0	7,9	27%
Sri Lanka	1	-		0,00%	-	-	0%	1	-	0%	-	-	0%
Switzerland	462	266	58%	0,24%	71	12	17%	6	-	0%	9,0	4,0	44%
The former Yugoslav Republic of Macedonia	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Turkey	8 405	5 625	67%	4,43%	318	210	66%	380	-	0%	9,0	4,0	44%
Ukraine	8	2	25%	0,00%	1	-	0%	-	-	0%	-	-	0%
United Kingdom	20 127	13 894	69%	10,62%	4 476	3 290	73%	144	52	36%	306,0	144,3	47%
USA	80 703	63 147	78%	42,58%	29 707	23 646	80%	2 879	2 203	77%	1 577,0	1 237,9	78%
Total excluding USA	**108 829**	**64 901**	**60%**		**23 242**	**11 178**	**48%**	**1 353**	**285**	**21%**	**1 113,0**	**427,5**	**38%**
Total including USA	**189 532**	**128 048**	**68%**	**100%**	**52 949**	**34 824**	**66%**	**4 232**	**2 488**	**59%**	**2 690,0**	**1 665,4**	**62%**

5.2 Politiques et rapports de transparence des fournisseurs de services : sources

5.2.1 Apple

http://www.apple.com/legal/privacy/en-ww/
http://images.apple.com/privacy/docs/legal-process-guidelines-emeia.pdf
http://www.apple.com/privacy/transparency-reports/

5.2.2 Google

https://www.google.com/transparencyreport/
https://www.google.com/transparencyreport/removals/government/?hl=en
https://www.google.com/transparencyreport/userdatarequests/?hl=en

5.2.3 Facebook

https://govtrequests.facebook.com/

5.2.4 Microsoft

https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/
https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr/
https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/crrr/

5.2.5 Twitter

https://support.twitter.com/articles/41949#
https://transparency.twitter.com/

5.2.6 Yahoo

https://transparency.yahoo.com/
https://transparency.yahoo.com/law-enforcement-guidelines/us

5.2.7 Other references and links[63]

Adobe
Law enforcement guide:
https://www.adobe.com/legal/compliance/law-enforcement.html
Transparency report:
https://www.adobe.com/legal/compliance/transparency.html

Amazon
Law enforcement guide:
http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf
Transparency report:
http://d0.awsstatic.com/certifications/Transparency_Report.pdf
Privacy notice:
http://www.amazon.com/gp/help/customer/display.html?nodeId=468496
Conditions of use:
https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088
Privacy and data security blog post:
http://blogs.aws.amazon.com/security/post/Tx35449P4T7DJIA/Privacy-and-Data-Security

[63] Established by the Electronic Frontier Foundation: Who has your back? Protecting your data from government requests https://www.eff.org/who-has-your-back-government-data-requests-2015

Apple
Law enforcement guide:
https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf
Transparency report:
https://www.apple.com/privacy/transparency-reports/
Government information requests:
https://www.apple.com/privacy/government-information-requests

AT&T
Law enforcement guide:
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/location-demands.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/emergency-requests.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/international.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html
Transparency report:
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html#sthash.BMut0WAH.dpuf

Comcast
Law enforcement guide:
http://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx
Transparency report:
http://corporate.comcast.com/images/Third-Comcast-Transparency-Report-2H2014-FINAL-02022015.pdf
Privacy notice:
http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html?CCT=53BA3D76CB1473BFF49C79FE4AA86DFF1EE2DE626F409A592CC8FD4F97F987FDED44763A4B54572047B30DDBC6AEBC5DCED6A73183C574B8E5697D9E3FD17293EB4FE71DF37B56C34FF77B9D0E092477A8C3958E8CC866906A7E34373B5718A30AEEF8F52C31E24CFFD314BC83C96E756A5AA0BA63C22EB0#When%20is%20Comcast%20required%20to%20disclose%20personally%20identifiable%20information%20and%20CPNI%20by%20law?
Statement on Upgrading the Security and Privacy of Your Email:
http://corporate.comcast.com/comcast-voices/upgrading-the-security-and-privacy-of-your-email

CREDO Mobile
Law enforcement guide:
http://www.credomobile.com/law-enforcement-guidelines
Transparency report:

http://www.credomobile.com/transparency
Privacy and security policy:
http://www.credomobile.com/privacy

Dropbox Transparency report:
https://www.dropbox.com/transparency
Government Data Request Principles:
https://www.dropbox.com/transparency/principles

Facebook
Law enforcement guidelines:
https://www.facebook.com/safety/groups/law/guidelines/
Transparency report:
https://govtrequests.facebook.com/
Data policy:
https://www.facebook.com/full_data_use_policy

Google
Legal process:
https://www.google.com/transparencyreport/userdatarequests/legalprocess/
Transparency report:
https://www.google.com/transparencyreport/
Dashboard data:
https://support.google.com/accounts/answer/162743?hl=en
Government requests to remove content:
https://www.google.com/transparencyreport/removals/government/

LinkedIn
Law enforcement guidelines:
https://help.linkedin.com/app/answers/detail/a_id/16880/~/linkedin-law-enforcement-data-request-guidelines
Transparency report:
https://www.linkedin.com/legal/transparency
Data request guidelines:
https://help.linkedin.com/ci/fattach/get/4773861/1431363803/redirect/1/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf

Microsoft
Principles, policies, and practices FAQ (law enforcement guidelines and other information):
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/
Transparency report
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
U.S. National Security Order Requests:
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/fisa/
Privacy statement:
http://www.microsoft.com/privacystatement/en-us/core/default.aspx#EHC
When transparency alone isn't enough:
http://blogs.microsoft.com/on-the-issues/2015/03/27/when-transparency-alone-isnt-enough/

Pinterest
Law enforcement guidelines:
https://help.pinterest.com/en/articles/law-enforcement-guidelines
Transparency report:
https://help.pinterest.com/en/articles/transparency-report-archive
Terms of service:
https://about.pinterest.com/en/terms-service

reddit
Transparency report (including law enforcement guidelines)
https://www.reddit.com/wiki/transparency/2014
What information we collect:
https://www.reddit.com/help/privacypolicy#section_what_information_we_collect

Slack
User data request policy:
https://slack.com/user-data-request-policy
Transparency report:
https://slack.com/transparency-report
Slack and transparency:
http://slackhq.com/post/117871977170/transparency
FAQ about privacy policy:
https://slack.zendesk.com/hc/en-us/articles/203950296-FAQs-about-Slack-s-Privacy-Policy
Privacy policy:
https://slack.com/privacy-policy

Snapchat
Law enforcement guidelines:
https://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604
Transparency report:
http://blog.snapchat.com/post/115310648870/our-transparency-report

Sonic
Law enforcement guidelines:
https://wiki.sonic.net/images/0/05/Sonic.net_Legal_Process_Policy.pdf
Transparency report:
https://corp.sonic.net/ceo/2014/04/28/2013-transparency-report/

Tumblr
Law enforcement guidelines:
https://www.tumblr.com/docs/en/law_enforcement
Transparency report:
https://www.tumblr.com/transparency

Twitter
Law enforcement guidelines:
https://support.twitter.com/articles/41949-guidelines-for-law-enforcement
Transparency report:
https://transparency.twitter.com/

Privacy policy
https://twitter.com/privacy?lang=en

Verizon
Transparency report and law enforcement guide:
http://transparency.verizon.com/us-report?/us-data
http://transparency.verizon.com/international-report

Wickr
Law enforcement guide
https://wickr.com/wp-content/uploads/2014/06/Law-Enforcement-Guidelines_5.12.14.pdf
Transparency report:
https://wickr.com/category/transparency-report/
Privacy policy:
https://wickr.com/privacy-policy/

Wikimedia
Law enforcement guide:
https://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines#What_We_Require_From_You
Transparency report:
https://transparency.wikimedia.org
https://transparency.wikimedia.org/content.html
Data retention guidelines:
https://meta.wikimedia.org/wiki/Data_retention_guidelines

Wordpress.com
Law enforcement guide:
https://en.support.wordpress.com/disputes/legal-guidelines/
Transparency report:
http://transparency.automattic.com/
Takedown demands:
http://transparency.automattic.com/takedown-demands/

Yahoo
Transparency report:
https://transparency.yahoo.com/
Law enforcement guide:
https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm
Content removals:
https://transparency.yahoo.com/government-removal-requests/index.htm
Users first statement:
https://transparency.yahoo.com/users-first/index.htm